GN-WS33N-RH
802.11 b/g/n Mini Card

Quick Start Guide

http://www.gigabyte.com.tw

Rev. 1.0

Federal Communication Commission Interference Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:
To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

IMPORTANT NOTE
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:
This module is intended for OEM integrator. The OEM integrator is still responsible for the FCC compliance requirement of the end product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

USERS MANUAL OF THE END PRODUCT:

In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users manual: This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

LABEL OF THE END PRODUCT:

The final end product must be labeled in a visible area with the following " Contains TX FCC ID: **JCK-GN-WS33N-RH** ". If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label: This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Contents

Chapter 1 Product Overview

1.1 Introduction to the 802.11 b/g/n Mini Card

This GN-WS33N-RH 802.11b/g/n Wireless Local Area Network (WLAN) PCI-Express Half Mini-card adapter is composed of the MAC, Baseband, and radio components, PCI-Express half mini-card interface, and two RF connectors with high throughput feature. It operates at 2.4GHz frequency band, providing fast (receive up to 150/300Mbps) and secure (WEP 64/128, WPA and WPA2) connections to 802.11n networks from a single adapter. It is backward compatible with 11b and 11g. GN-WS33N-RH overcomes environment multi-path effect by multi-input feature and to keep its stable wireless performance and running wireless anywhere.

1.2 Features

- Conform to IEEE 802.11b, 802.11g and draft 802.11n specification
- Wireless transmits/receive data rate up to maximum speed of 150/300Mbps
- Dynamically scales the data rate
- Support 64/128-bit WEP encryption, 802.1x, WPA and WPA2
- Support Quality of Service WMM
- Automatic power management to reduce battery consumption
- Seamless roaming between 11b, 11g and draft 11n networks

1.3 Product Specifications

System Specifications

System	
Host Interface	**PCI Express Mini Card v1.0**
Chipset	**Ralink MAC/BB/RF RT3091**
Operating Voltages	**3.3V+/-5%**
Typical Power	**Transmitting (Legacy mode): 280mA by 3.3V, 92mA by 1.5V@ 11b, 290mA by 3.3V, 125mA by 1.5V@ 11g; Transmitting (HT20 mode): 285mA by 3.3V, 125mA by 1.5V; Transmitting (HT40 mode): 290mA by 3.3V, 125mA by 1.5V; Receiving (Legacy mode, HT20): 130mA by 3.3V, 170mA by 1.5V @ 11b/g; Receiving (HT40 mode): 160mA by 3.3V, 170mA by 1.5V.**
RF – 802.11n (backward compatible to 802.11g & 11b)	
Frequency Band	**2412 ~ 2484 MHz (subject to local regulation)**
Modulation Technology	**OFDM and DSSS**
Modulation Techniques	**64QAM, 16QAM, QPSK, BPSK, DBPSK, DQPSK, CCK**
Data Rates	**Transmit up to 150Mbps and auto fallback Receive up to 300Mbps**

Output power	**Legacy mode: 18 dBm @11Mbps, 14 dBm @54Mbps; HT20 mode: 14 dBm @MCS7 (72.2Mbps); HT40 mode: 14 dBm @MCS7 (150Mbps).**
Receive Sensitivity	**Legacy mode: -90 dBm @11b, -77 dBm @11g; HT20 mode: -72 dBm @ MCS7/15; HT40 mode: -70 dBm @ MCS7/15.**
Antenna	**Two RF connectors**
Regulatory and Environmental Compliance	
EMC certification	**FCC part 15 (USA)**
Temperature Range	**Operating: 0 ~ 65 degree C, Storage: -20 ~ 65 degree C**
Humidity	**10% ~ 85% Non-condensing**
Software	
Driver	**Windows 2000/XP/Vista**
Security	**64/128 bit WEP, WPA and WPA2**
Quality of Service (QoS)	**WMM**
Roaming	**Seamless roaming among 11b/g/n access points.**
Management Utility	**Monitors the network situation.**
Mechanical	
Weight	**4.0 g ± 1.0g**
Dimension	**29.85 *26.7*3.3 mm ± 0.15mm**
Packaging	**Generic, Gigabyte, private labeling optional**

Subject to be changed without notices.

Chapter 2 Installation

2-1. SmartSetup 3

Note: The following section applies to users of GIGABYTE Wireless Routers.

GIGABYTE SmartSetup 3 is a powerful, yet user-friendly wireless network configuration wizard specially designed for GIGABYTE wireless networks. If you are connecting to a GIGABYTE wireless router, SmartSetup 3 will detect this and activate.

In three easy steps, you can establish a bulletproof WPA(WPA-PSK) wireless network AND configure your Internet connection. Only GIGABYTE delivers this easy, powerful and secure solution for your wireless network!

Step 1: Select the GIGABYTE wireless router from the available networks.

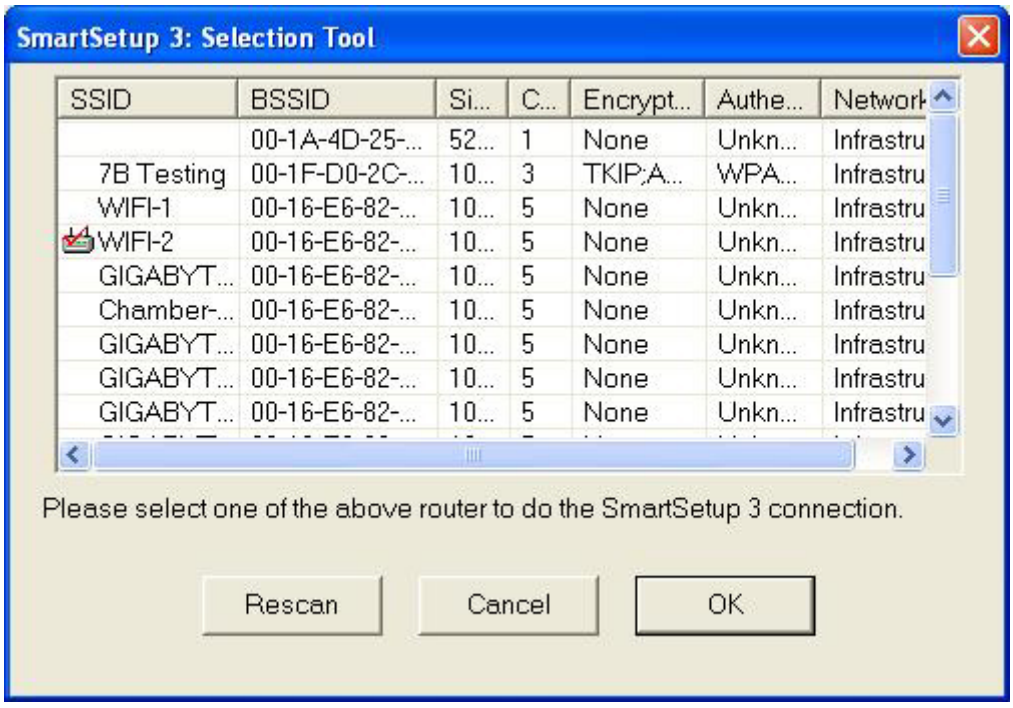

Figure 2-5. SmartSetup 3 Network Selection

Step 2: Create a WPA(WPA-PSK) Passphrase using any keyboard character. Make it no less than 8 but no more than 63 characters in length. Anyone wishing to gain access to your network, will first need to key-in this Passphrase. In the example below, we used ‘I love green eggs and ham’.

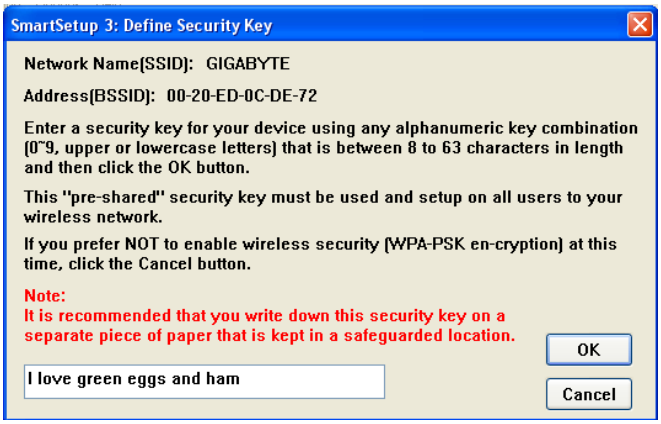

Figure 2-6. SmartSetup 3 Define Passphrase

Step 3: Your GIGABYTE router's web configuration utility will automatically open, and detect your ISP type. Just input the Username and Password. Click **Continue.**

Figure 2-7. Auto detecting your ISP type

Note: *If Figure2-7 Setup" from the main menu which displays. For more information about SmartSetup 3, please see the enclosed* ***Quick Start Guide.***

Chapter 3 Using the Wireless Utility

***Please note that Gigabyte Wireless Utility does not support Windows Vista operating system.**

The GN-WS33N-RH Wireless Utility is a powerful application that helps you to configure the Adapter and monitor the statistics of the communication link. It also permits the configuration for parameters while the Adapter is operating – no restarting is required. It also offers more configuration options than does Windows native Zero Wireless Configuration. It appears as the "G" icon in the task bar at the bottom right corner of screen whenever the Adapter is in operation *(see **Figure 3-1**)*. The quick start icon also doubles as a signal strength monitor, as indicated by its four small green lights.

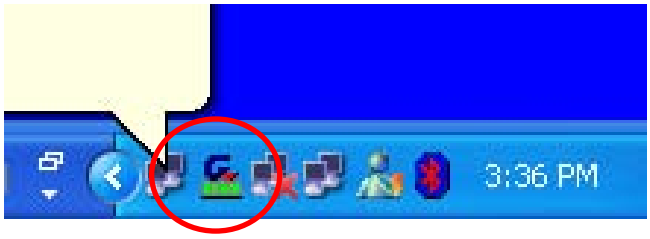

Figure 3-1. GN-WS33N-RH Wireless Utility quick start icon

To open the GN-WS33N-RH Utility, double click the quick start icon located in your system tray. Or, go to Windows **Start** menu, select **Programs, Gigabyte Wireless Network Adapters, GN-WS33N-RH** and then **GN-WS33N-RH Utility**.

Note: You may only use the utility to change wireless configurations when the GN-WS33N-RH is enabled and operating. You have to use Windows native Zero Configuration tool provided with Windows when the Adapter is not enabled.

Opening the GN-WS33N-RH Wireless Utility, you are presented with the Profile Tab. There are 5 main tabs with which to control and monitor your GN-WS33N-RH – Profile, Link, Site Survey, Statistics and the About Tab. The following sections will cover each tab in detail.

3.1. Profile Tab

The **Profile** tab shows you the current association information about the profile. *(*see ***Figure 3-2****)*. Profiles are useful if you often associate with different access points. You can configure a group of settings depending on the access point you often associate with and save as a profile, Click the **Add** button to create a new profile (see section below for further details), the **Delete** button to delete a selected profile, the **Edit** button to modify a selected profile and click the **Activate** button to have a selected profile become active.

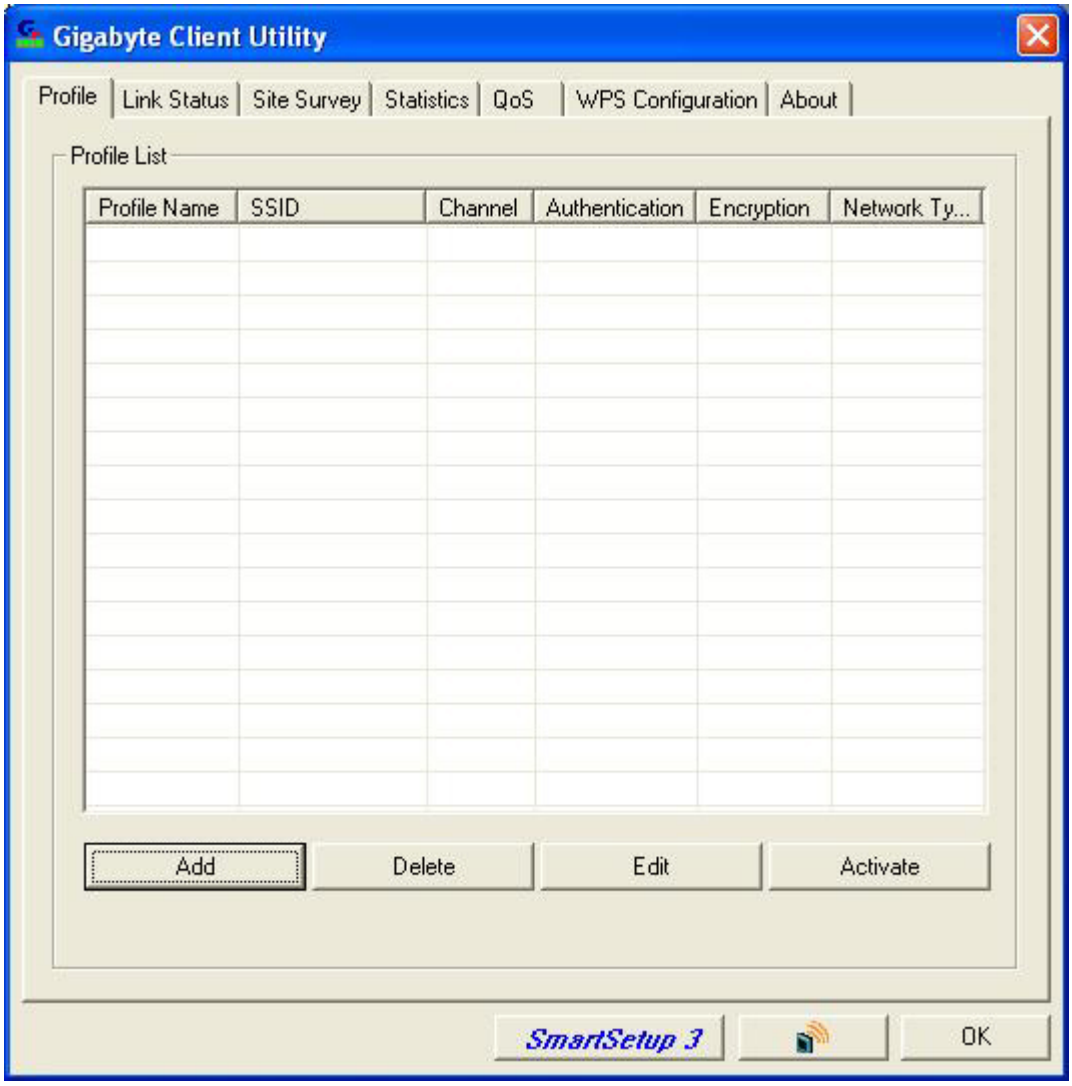

Figure 3-2. Current profile

Description of items in ***Figure 3-2*** is as follows:

Profile Name: A profile can be saved for various wireless settings in different environments, i.e. home, office, and the corner coffee shop.

SSID: The Network Name of the wireless router or Access Point.

Channel: Shows the current wireless channel.

Authentication: Sever authentication types. They include “OPEN”, “Shared”, “LEAP”, “WPA”, “WPA-PSK”, “WPA2” and “WPA2-PSK”.

Encryption: The type of encryption used in this profile: “None”, “WEP”, “AES” and “TKIP”.

Network Type: Informs you if an Access Point (infrastructure) or Ad Hoc is connected. In Ad Hoc, you may select a channel for each member participating in Ad Hoc.

3-1-1. Configuration Screen

If you want to **ADD** new profiles, or **EDIT** existing ones, the Configuration screen will open. Here you will Name your profile, and if you like, select an alternate network type (Ad hoc), restrict on SSID connections and more. All three tabs shown (see ***Figure 3-3)*** are related, so when you're done with all three (Configuration, Authentication, Advanced) tabs, click **OK.**

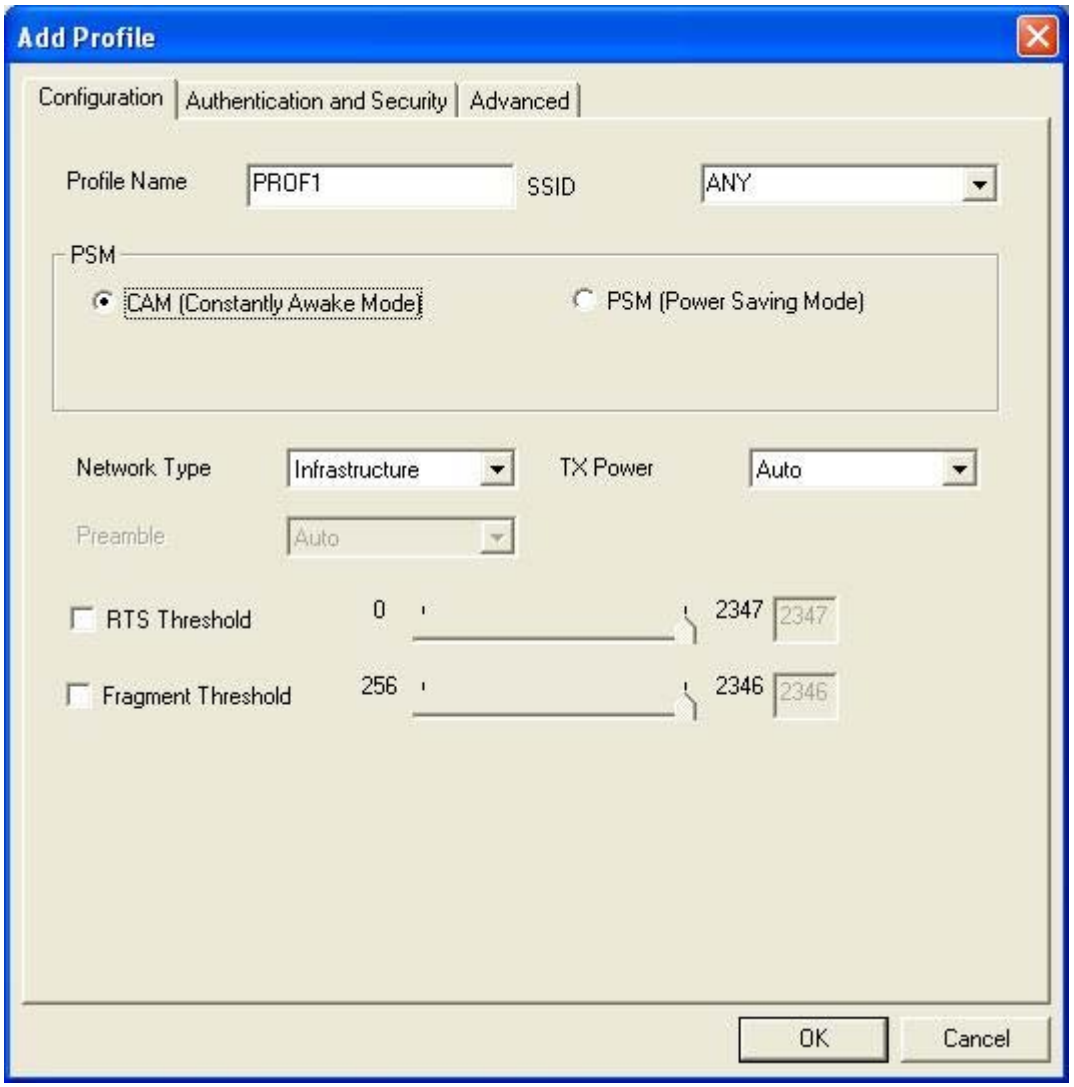

Figure 3-3. Configuration

Description of items in ***Figure 3-3*** is as follows:

Profile Name: Users can save different profiles names for different configurations.

SSID: Select the AP detected by the system from the drop-down menu or input a SSID. (Default: ANY)

Power Saving mode: Select "Power Saving Mode" (PSM) to turn off the Adapter's transceiver when not in use, or select CAM to continuously turn on transceivers. (Default: OFF)

Network Type: "Infrastructure" and "Ad Hoc". When Infrastructure network type is chosen, PSM will function but not Preamble. On the contrary, when Ad hoc type is chosen,

Preamble will function but not PSM. Also, the Channel option will appear and 802.1X Authentication will be disabled. (Default: Infrastructure)

TX Power: Select percentage of transmitted power. (Default: Auto)

RTS Threshold: This is a mechanism implemented to prevent the “Hidden Node” problem, “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other and can not detect each other. This mechanism is a way to prevent data collision when Adapters require transmission. (Default: OFF)

Fragment Threshold: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. (Default: OFF)

3-1-2. Authentication and Security Screen:

If an authentication or security setting is configured in your Access Point or router, you must enable this function to ensure successful connection. Use the following tab to configure data security and ID authentication (see ***Figure 3-4***). You may configure different settings in the profile, including 802.11 Protocol Authentication and Security and 802.1X Protocol.

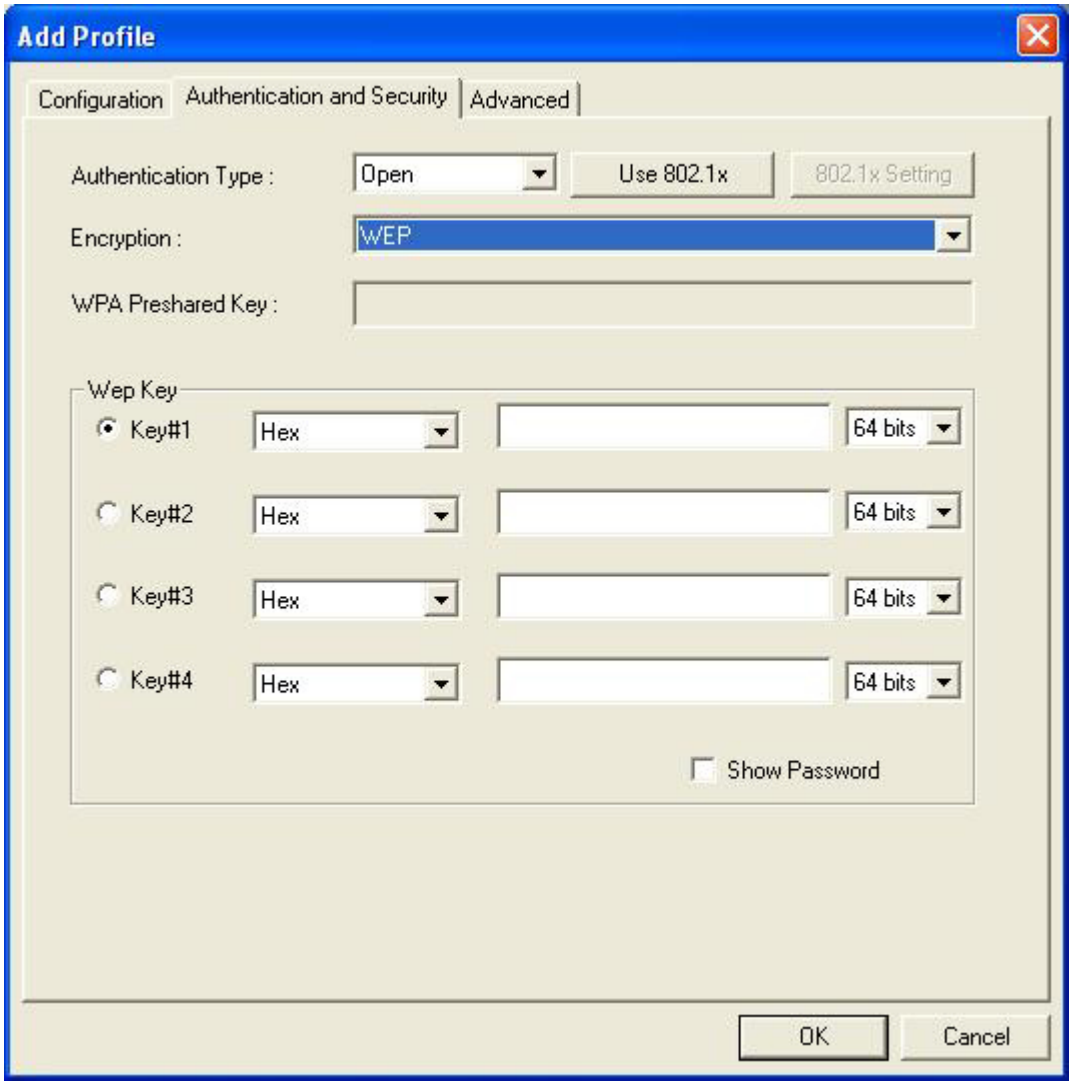

Figure 3-4. Authentication and Security

Authentication Type: Before a station connects to a SSID, the authentication type used by the SSID must be known. Authentication types include OPEN SYSTEM, WPA, WPA-PSK, WPA2, WPA2-PSK, LEAP and SHARED.

Encryption: To prevent unauthorized access to data transmitted on the network, the Adapter and the Access Point agree on a type of data encryption. Any station that wishes to connect must have the same password and encryption scheme to connect. Different authentication types have different level of security. (Default: TKIP)

WEP encryption: Select one of the four keys as the default encrypted key.

To setup WEP, you will need to set a ASCII or HEX key to connect to Access Point. The WEP Key can only be saved through the setting of profile.

1. Select a Key #.
2. Select a form of the key (Hex or ASCII).
3. Enter password. Please enter 26 hexadecimal digits or 13 ASCII digits.
4. Click OK to save the settings.

Making HEX keys:
64-bit - Generated as 10 alphanumeric characters (0-9, a-f) (example: 843c29a562)
128bit - Generated as 26 alphanumeric characters (0-9, a-f) (example: 3c29f2536bef3276d32e364a2c)

Note: Using a Hex key is more secure than using an ASCII key, and if you are connecting to a GIGABYTE Router or Access Point, ASCII keys are not allowed and you **must** use a Hex key.

WPA-PSK/WPA2-PSK encryption: WPA-PSK/ WPA2-PSK (Preshared Key) uses TKIP or AES based on your choice. You create a password (or Passphrase as its often called) and the system will use the Passphrase to create a cipher code in which it will encrypt the data.

To use WPA-PSK/ WPA2-PSK:

1. Create a Passphrase, and key it in. Use 8~63 ASCII digits.
2. Remember this Passphrase. If you forget the Passphrase, you will have to do a hard reset of the Access Point in order to restore default settings and connect again.
3. Click “OK to save these settings.

3-1-2-1. 802.1X Setting - Certification Tab

Clicking **Use 802.1X Authentication** and then **Enter 802.1X configuration** from the Authentication and Security Window will bring up the 802.1x Setting Window and the **Certification Tab (***see* ***Figure 3-5).***

From the Certification screen, you may configure information about authentication, such as Tunnel Protocol, ID and Password and Client Certificate or Certificate Chain. *(see* ***Figure 3-5 and 3-7****)*

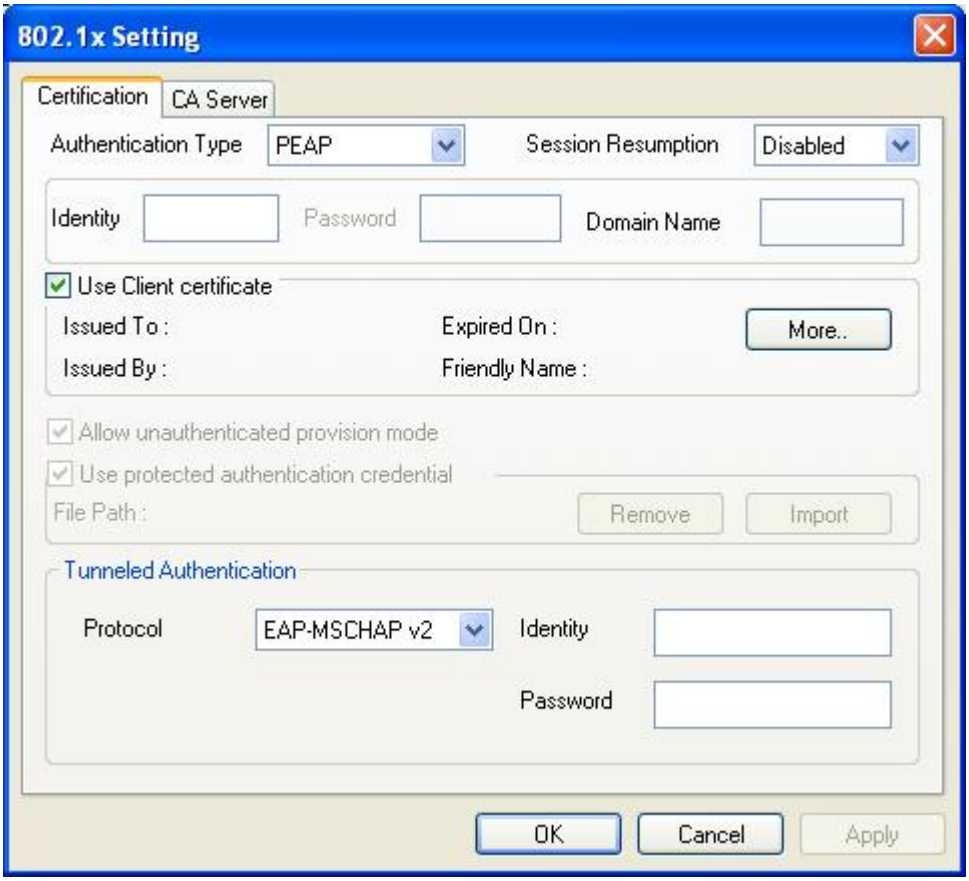

Figure 3-5. 802.1X Authentication

Description of items in ***Figure 3-5*** is as follows:

Authentication type: PEAP, TLS/Smart Card, TTLS and MD5-Challenge. (Default: PEAP)

Session Resumption: This feature can create a new connection without the overhead of a full handshake.

Identity: The Account's User ID.

Password: Passwords for users accounts can be used when LEAP and MD5-Challenge are selected as authentication types.

Use Client Certificate: This certificate is necessary for TLS and an option for PEAP and TTLS. Check "Use Client Certificate" to verify the authenticity of a Client Certificate during the authentication process.

Clicking **More** will open the **Client Certificate Selection** Window (shown in ***Figure 3-7***). Users can select one suitable certificate as Client Certificate. (Default: OFF)

Tunnel Authentication: PEAP and TTLS use two-step authentication method. The first step is that Server sets up a Tunnel with its authentication. No option is need to be set for Client (the PC with the Adapter). The second step is to confirm the validity of Client with assigned authentication type in the Tunnel. Data needed for authentication includes Tunnel ID, Tunnel Password, Client Certificate or Server Authentication.

Protocol: Use assigned authentication type in the safe tunnel.

Tunnel ID: Users' accounts.

Password: Passwords for users' accounts.

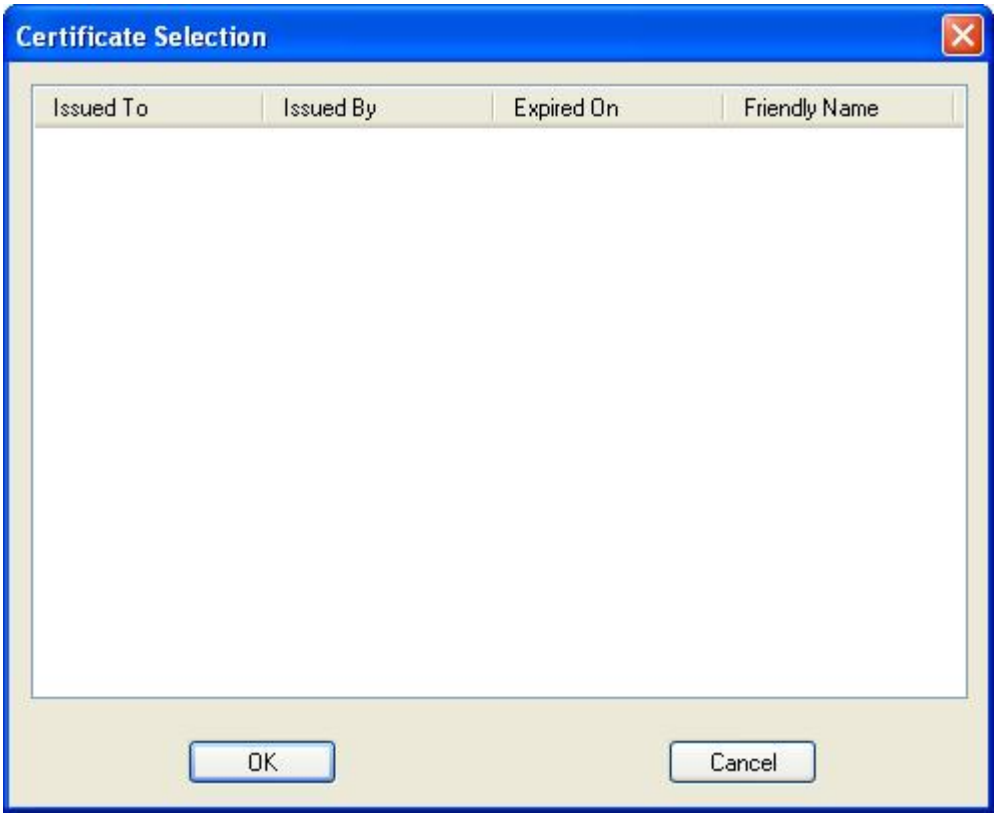

Figure 3-6. Client Certificate Selection List

3-1-2-2. 802.1x Settings - CA Server Tab

CA Server is used when TLS, TTLS or PEAP is in use. When **Use certificate chain** is checked, the Client can verify if such server is reliable and then transmit Client Certificate after the verification is confirmed.

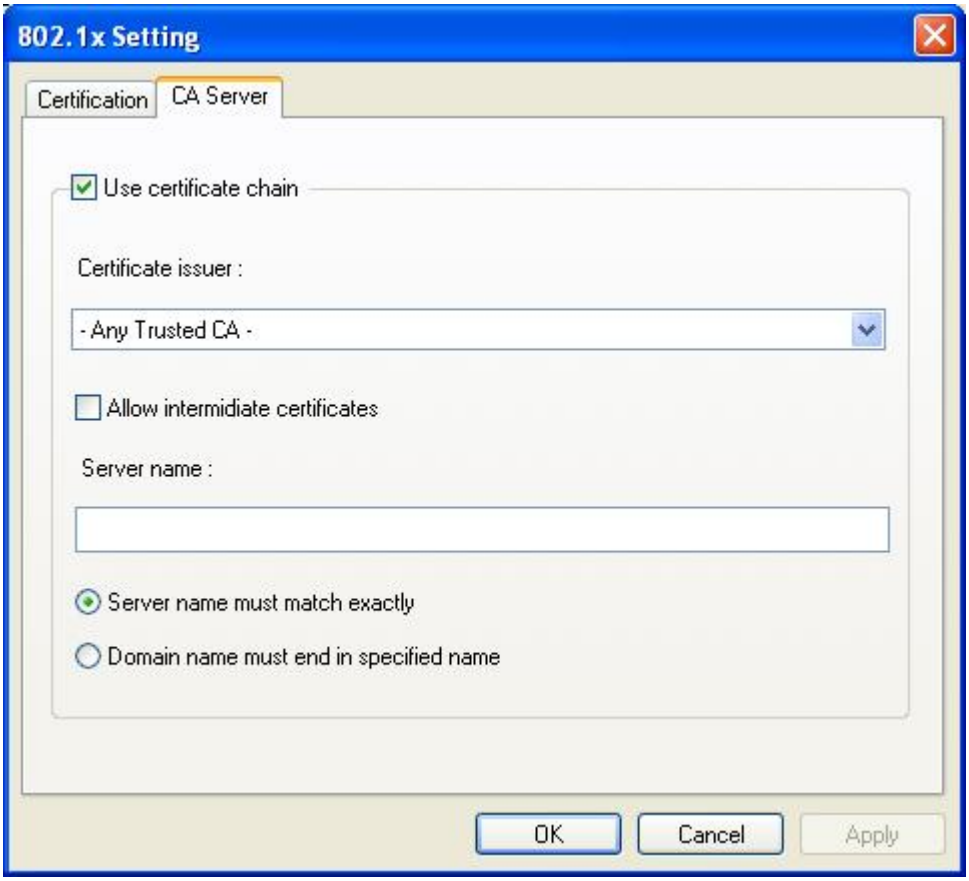

Figure 3-7. CA Server Setting

To verify the CA server:

1. Confirm if the Server Certificate is issued by assigned certificate issuer. If “Allow Intermediate Authentication” is checked, the server certificate can be issued by one intermediate certificate issuer.

2. Check the server name of server certificate is the same as the name entered by the user or belongs to the same domain.

Use certificate chain: If “Use certificate chain” is checked, it indicates that Client will confirm whether CA server is reliable. (Default: OFF)

Certificate issuer: CA of a server certificate can be selected from certificate issuers on the drop-down list. (Default: ANY)

Allow intermediate Certificates: When this option is checked, the certificate issuer can be an issuer recognized by a specific certificate issuer. On the other hand, the server certificate must be issued by a certificate issuer selected by the user.

Server name: This value can be a server name or the name of a domain where the server is located.

Server name must match exactly: If this option is selected, the server name of server certificate must be the same as “Server Name” or as the name of domain where the server is located.

Domain name must end in specified name: If this option is selected, the certificate issuer must be the domain or secondary domain entered in “Server Name”.

3-1-3. Advanced Screen

The **Advanced** screen is the third tab in the trio of tabs under Edit Profile *(see **Figure 3-8**)*. It includes the 802.11b/g/n wireless transmission mode settings. Once you have finished configuration, just click **OK**. Then you will return to the Profile Tab (***Figure 3-2)***. A reboot is **not** needed for changes to take effect.

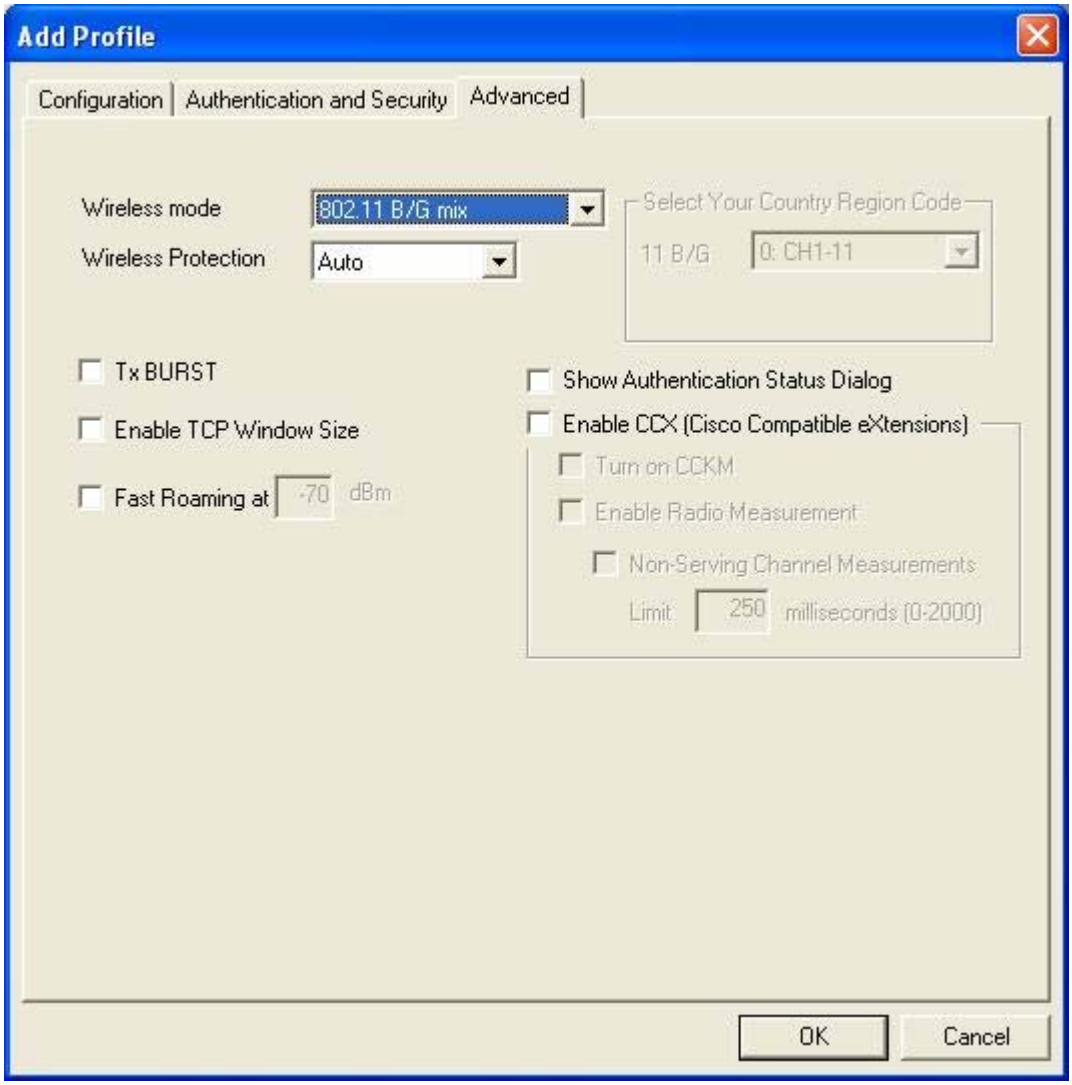

Figure 3-8 Advanced

Description of items in ***Figure 3-8*** is as follows:

Wireless Mode: Sets infrastructure Protocols, including 802.11 B/G mix and 802.11 B Only. (Default 802.11 B/G mix)

Ad Hoc Wireless Mode: Sets Ad Hoc Wireless Protocols, including 802.11 B/G mix, 802.11 B Only and 802.11 G Only. (Default: 802.11 B/G mix)

TX Burst: The longest interval between frames is normally one DIFS while frames are transmitted. When this setting is open, the longest interval between frames is one SIFS that means the system is allowed to transmit higher capacity of data in one interval.(Default: OFF)

B/G Protection: 802.11b uses CCK modulation. 802.11g uses OFDM while CCK modulation for 802.11b is compatible. To prevent data collision between two stations with 802.11b and 802.11g within range of the same Access Point, it is necessary to set 11B/G Protection. This setting only functions when 802.11 B/G mix is selected as Wireless Mode. Three setting are available: AUTO, ENABLE and DISABLE.

This is a mechanism implemented to prevent the “Hidden Node” problem, “Hidden Note” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other and can not detect each other. This mechanism is a way to prevent data collision when WLAN equipments require transmission. (Default: Auto)

TX Rate: This option adjusts settings of TX Rate according to the setting of “Infrastructure Wireless Mode. (Default: Auto)

3.2. Link Status Tab

The **Link Status** tab displays the current association information about the Adapters connection with a wireless network. *(see **Figure 3-9**)*

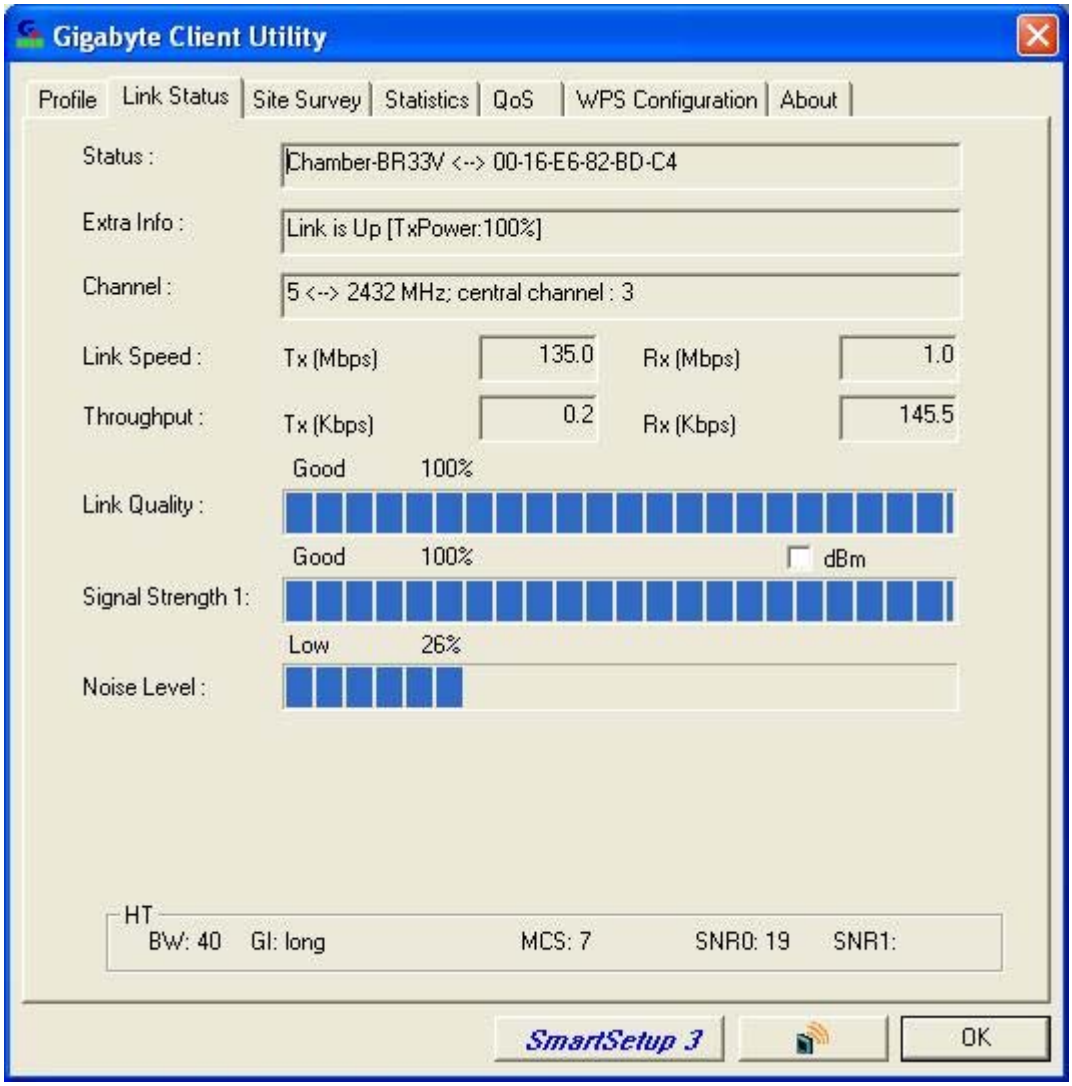

Figure 3-9. Link Status

Description of items in ***Figure 3-9*** is as follows:

Status: Shows current link status. “No Link” will appear on the screen when no connection is available. Otherwise, SSID and BSSID of a link will appear.

Channel: The current channel number used by the Adapter.

Link Speed: Transmission rate (transferring and receiving) at which data is transferred between Stations with Adapter and AP. The speed will adjust according to different modes (802.11b, 11g or mixed) and distance.

Throughput: Displays the transmitting (Tx) and receiving (Rx) bytes per second.

Link Quality: Measures quality of the link according to the quality of received AP signal.

Signal Strength: Measures signal strength received by RF signal processor and displays

the signal strength in dBm.

Noise Level: Noise level during connection.

3.3. Site Survey Tab

The **Site Survey** tab shows you the list of reachable access points and/or peer-to-peer Stations. Just double click on the SSID that you want to connect or click the **Connect** button. *(see **Figure 3-10**)*

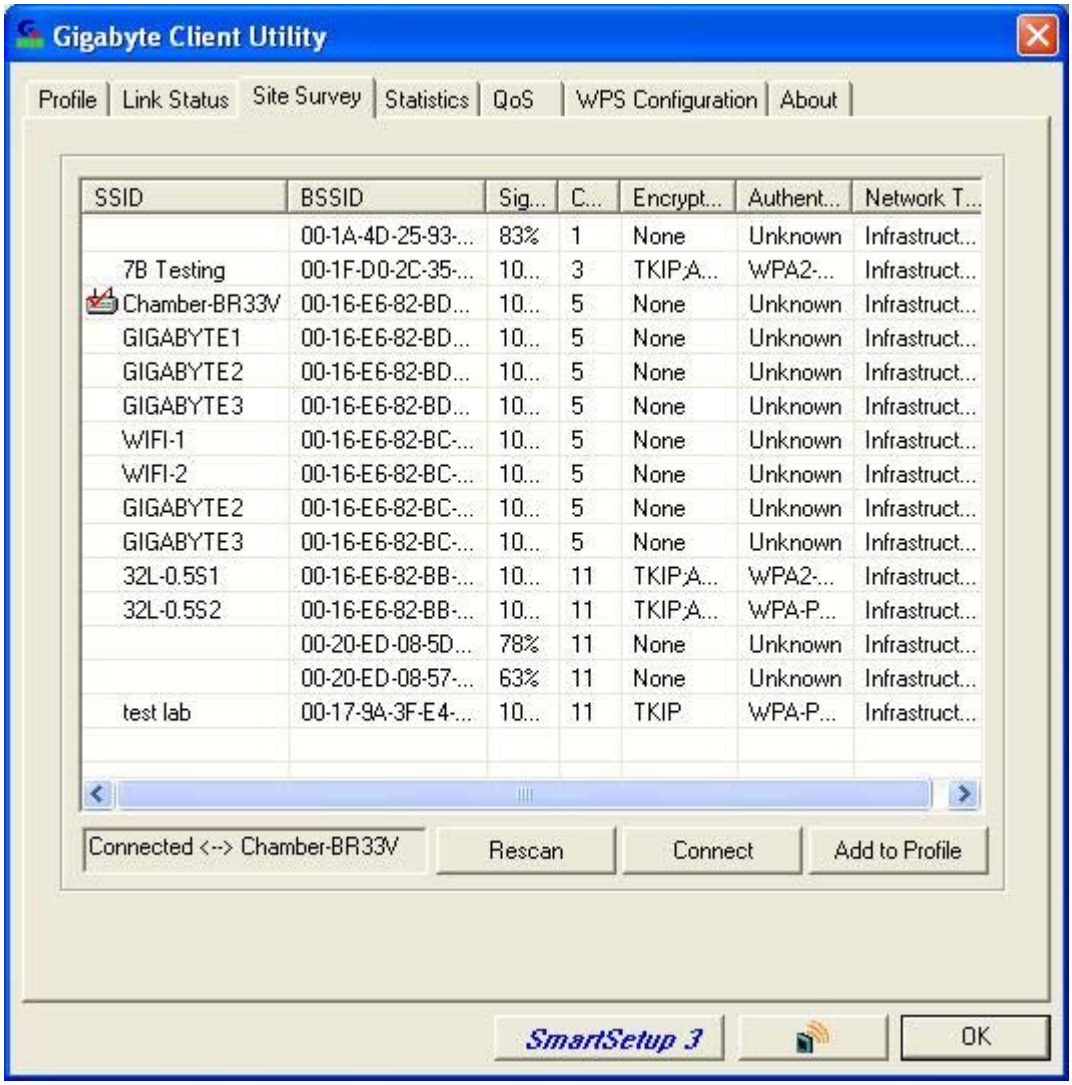

Figure 3-10. Site Survey

Description of items in ***Figure 3-10*** is as follows:

SSID: The name of the wireless network (also known as Network Name).

BSSID: Displays the MAC address of the Access Point or router.

Signal Strength: Displays the strength of the signal from a station to the AP.

Channel: Displays the current channel number used by the Access Point.

Encryption: The security method used by the Access Point.

Authentication: The authentication type used by the Access Point.

Network Type: Informs you if an Access Point (infrastructure) or other stations (802.11 Ad Hoc) is connected. When it is 802.11 Ad Hoc, we can select a channel for all members in 802.11 Ad Hoc.

Rescan: Rescan the available networks and then re-display results.

Connect: Connects with the highlighted Access Point.

Add to Profile: Adds a specific Access Point into the profile.

3.4. Statistics Tab

The **Statistics** tab shows you the number of packets sent and received by the Adapter *(see **Figure 3-11**)*

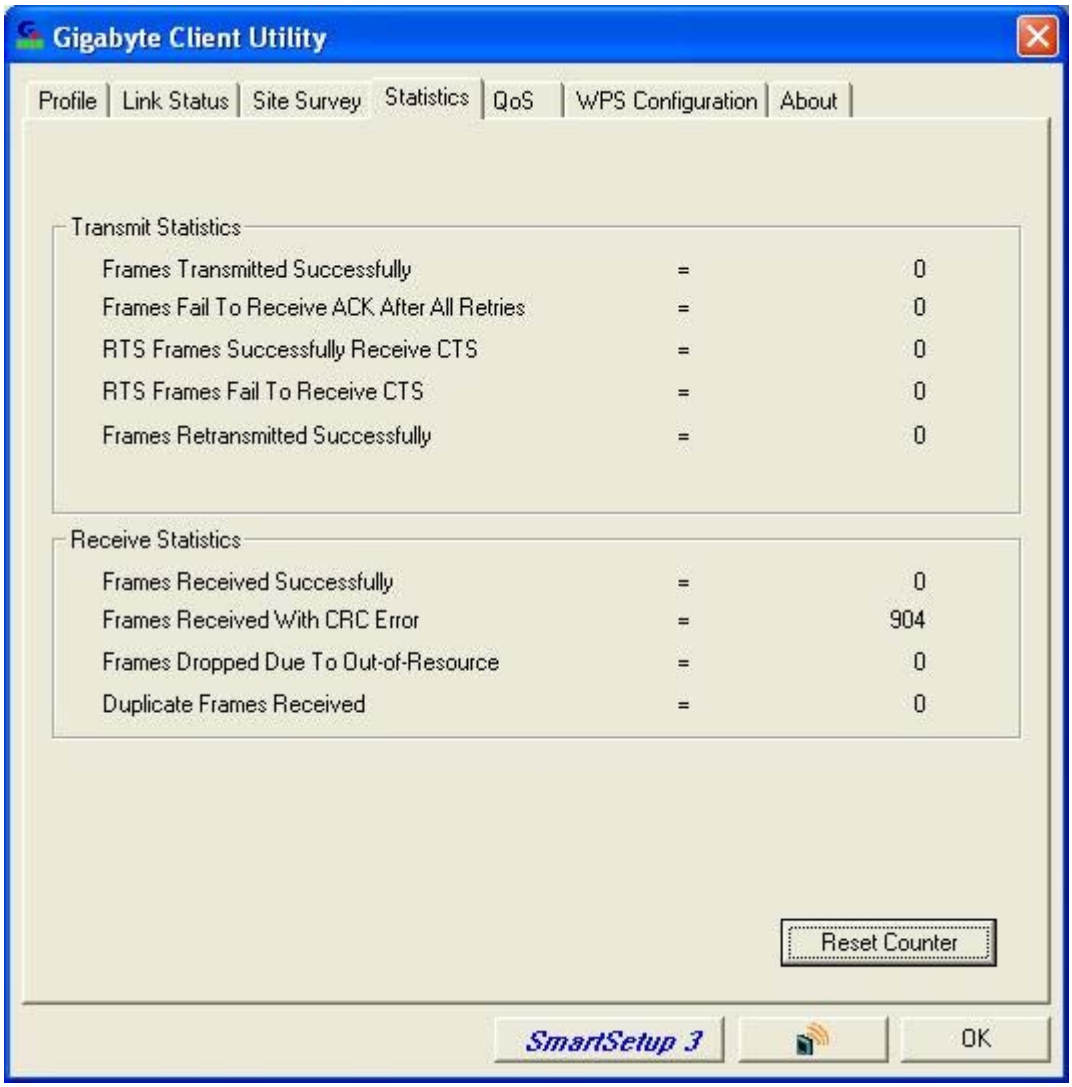

Figure 3-11. Statistics

Description of items in ***Figure 3-11*** is as follows:

Frames Transmitted Successfully: Number of frames transmitted successfully.

Frames Transmitted Successfully Without Retry: Number of frames transmitted successfully, excluding packets transmitted successfully with more than one retry.

Frames Transmitted Successfully After Retry[s]: Number of frames transmitted successfully with more than one retry.

Frames Fail To Receive ACK After All Retries: Number of frames failing to receive ACK after many retries.

RTS Frames Successfully Receive CTS: Number of RTS frames successfully received CTS (Clear To Send) from AP.

RTS Frames Fail To Receive CTS: Number of RTS frames fail to receive CTS from AP.

Frames Receive Successfully: Number of frames received successfully**.**

Frames Receive With CRC Error: Number of frames received with CRC Errors.

Frames Dropped Due TO Out-of-Resource: Number of frames dropped due to out-of-resource.

Duplicate Frames Received: Number of duplicate frames received.

Reset Counter: Resets the counter to zero.

3.5. QoS

The **Qos** tab allows you to configure the Quality of services settings. **Qos** configuration contains WMM Enable function, Enable WMM Power Save setting, and Enable Direct Link Setup. *(see **Figure 3-12**)*

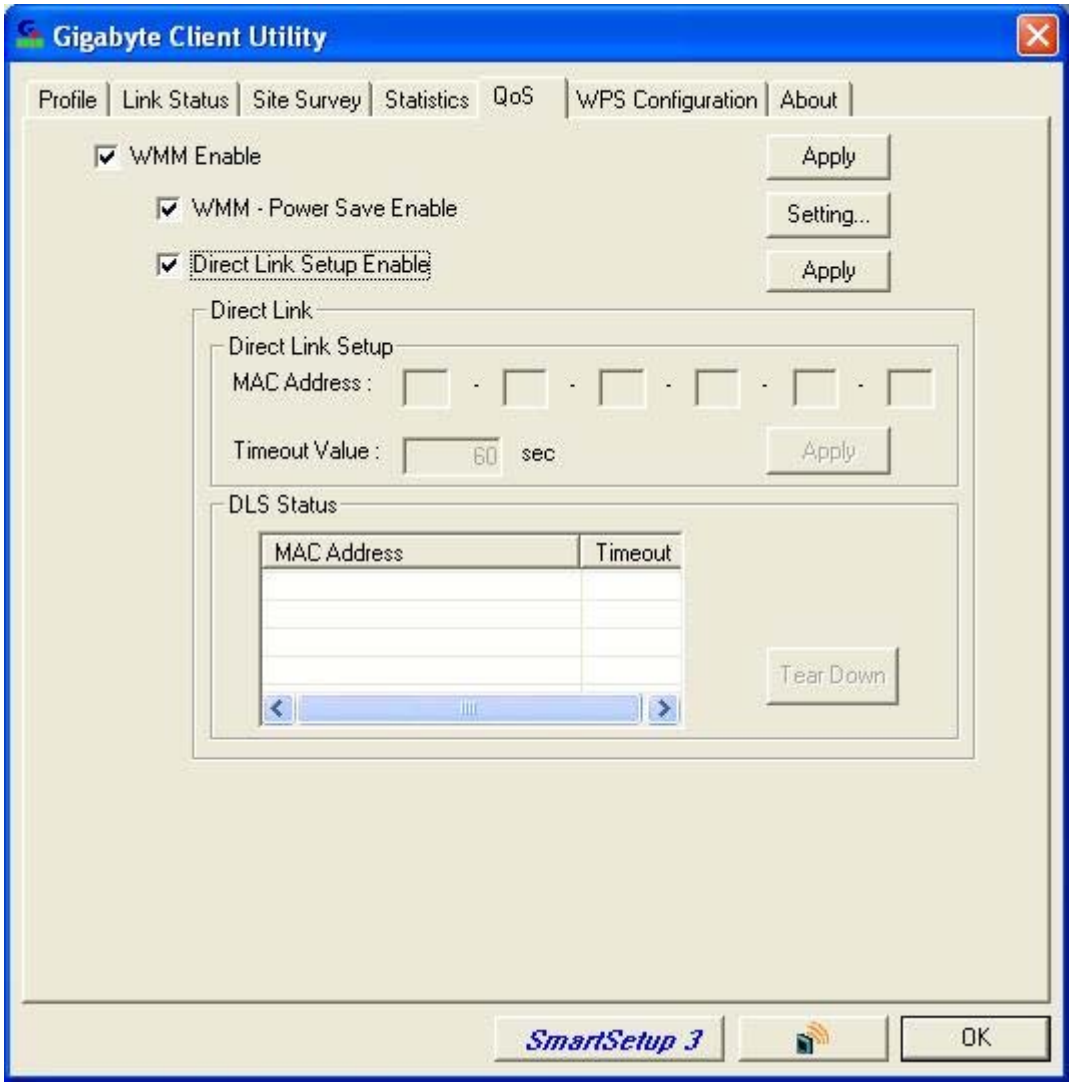

Figure 3-12. QoS Tab

WMM (Wi-Fi Multimedia) is a subset of the IEEE RFC known as 802.11e. WMM is designed to support user applications and works with all three 802.11 wireless physical layer standards - 802.11a, 802.11b and 802.11g. The specification provides basic prioritization of data packets based on four categories - voice, video, best effort and background.

WMM Power Save function can extend the battery life of Wi-Fi devices by increasing the efficiency and flexibility of data transmission. It is an addition to WMM technology that enables Quality of Service (QoS) functionality in Wi-Fi networks by prioritizing traffic from different applications.

WMM Enable– Enable Wi-Fi Multi-Media function. The following is setting method.

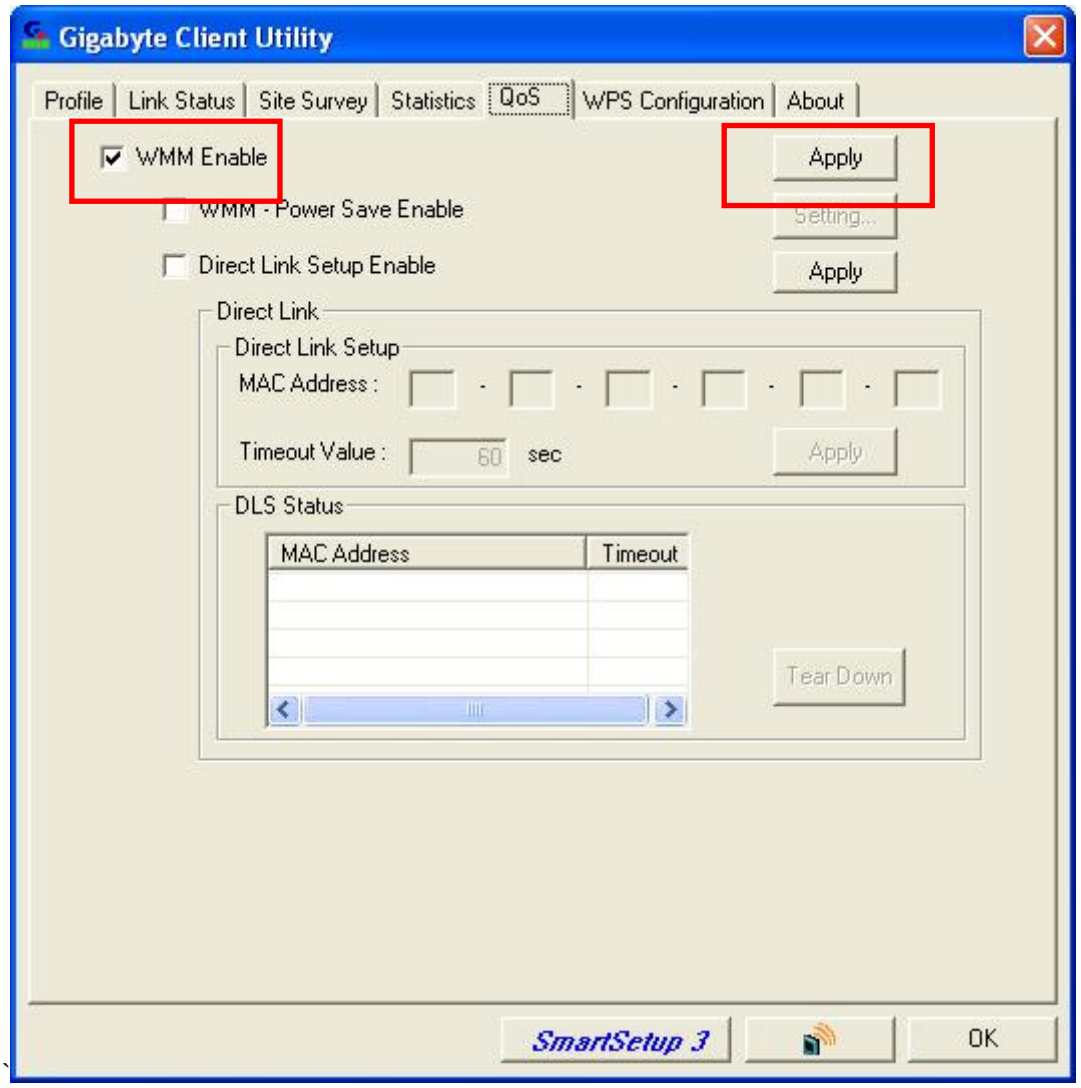

Figure 3-12-1. WMM Enable

Step 1. Click **WMM Enable**.
Step 2. Click **Apply**.
Step 3. Change to Site Survey Page. And add a AP that supports WMM features to a Profile.

WMM Power Save Enable– Enable WMM power save functions. Select WMM Power Save option and click Setting for further configuration which includes AC_BK, AC_BE, AC_VI, and AC_VO.

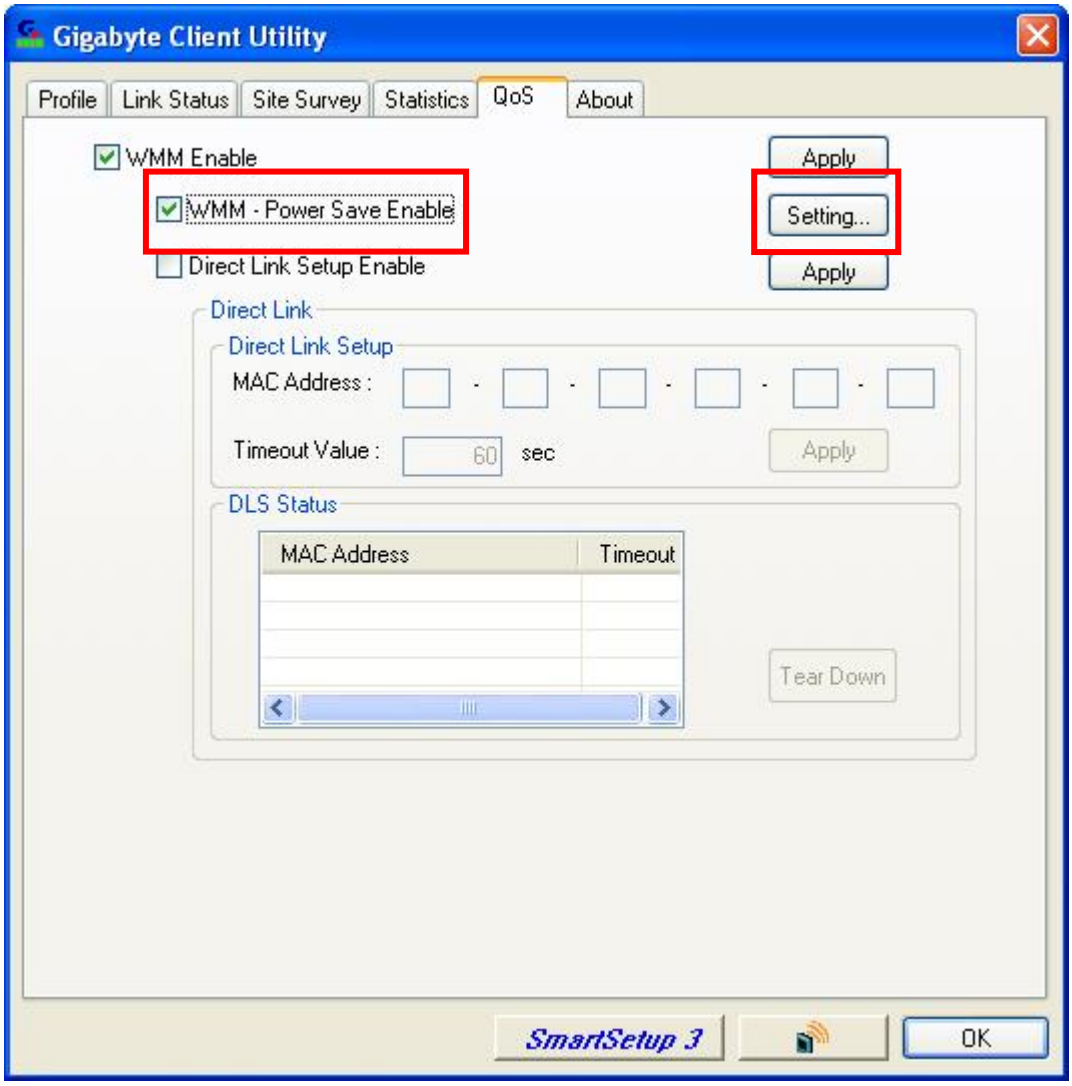

Figure 3-12-2. WMM Power Save Enable

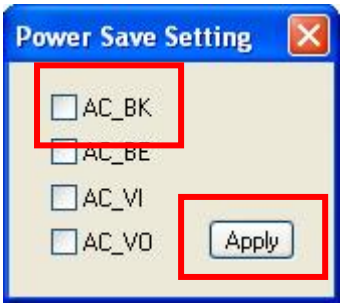

Figure 3-12-3. Power Save Setting

Step 1. Click **WMM- Power Save Enable** and click **Setting**.
Step 2. Pop up Power Save dialog box. Select ACs you wan to enable and click **Apply** button.

Direct Link Setup Enable– Enable Direct Link Setup Enable functions.

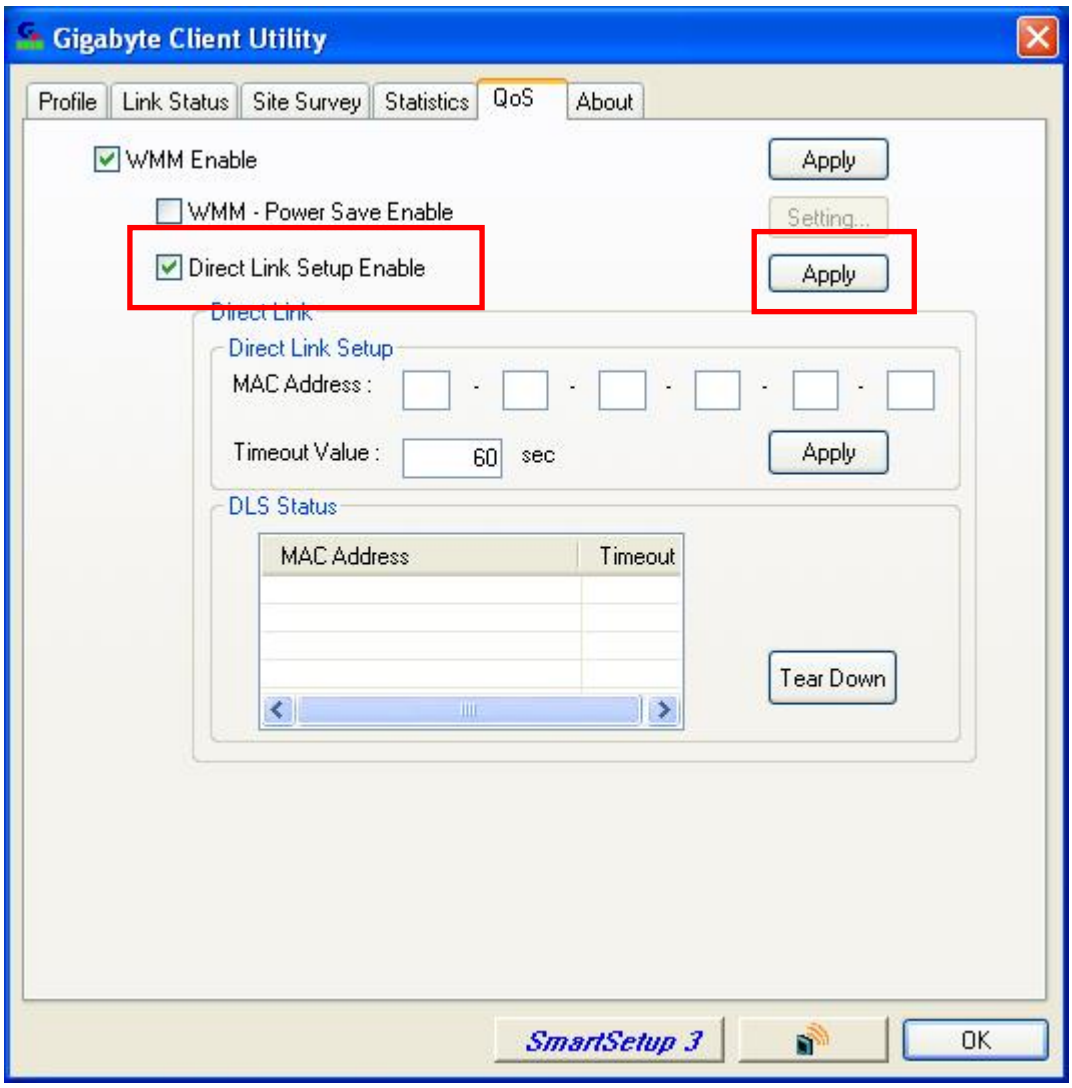

Figure 3-12-4. Direct Setup Enable

Step 1. Click **Direct Link Setup Enable**. And click **Apply** button.

Step 2. Change to Ste Survey Page. And add a AP that supports DLS features to a Profile.

Direct Link Setup MAC Address– Specify the MAC Address of client adapter you want to direct link and click Apply to add DLS status table.

Please note that to before enabling Direct Link Setup function, connect with the same AP that support DLS feature.

Timeout Value– Specify the timeout value for DLS.

DLS Status– DLS Status displays all DLS connections. If you want to terminate one of connections, just select specified connection and click Tear Down button.

3.6. About Tab

The **About** tab displays information about current drivers and physical MAC address *(see **Figure 3-13**)*.

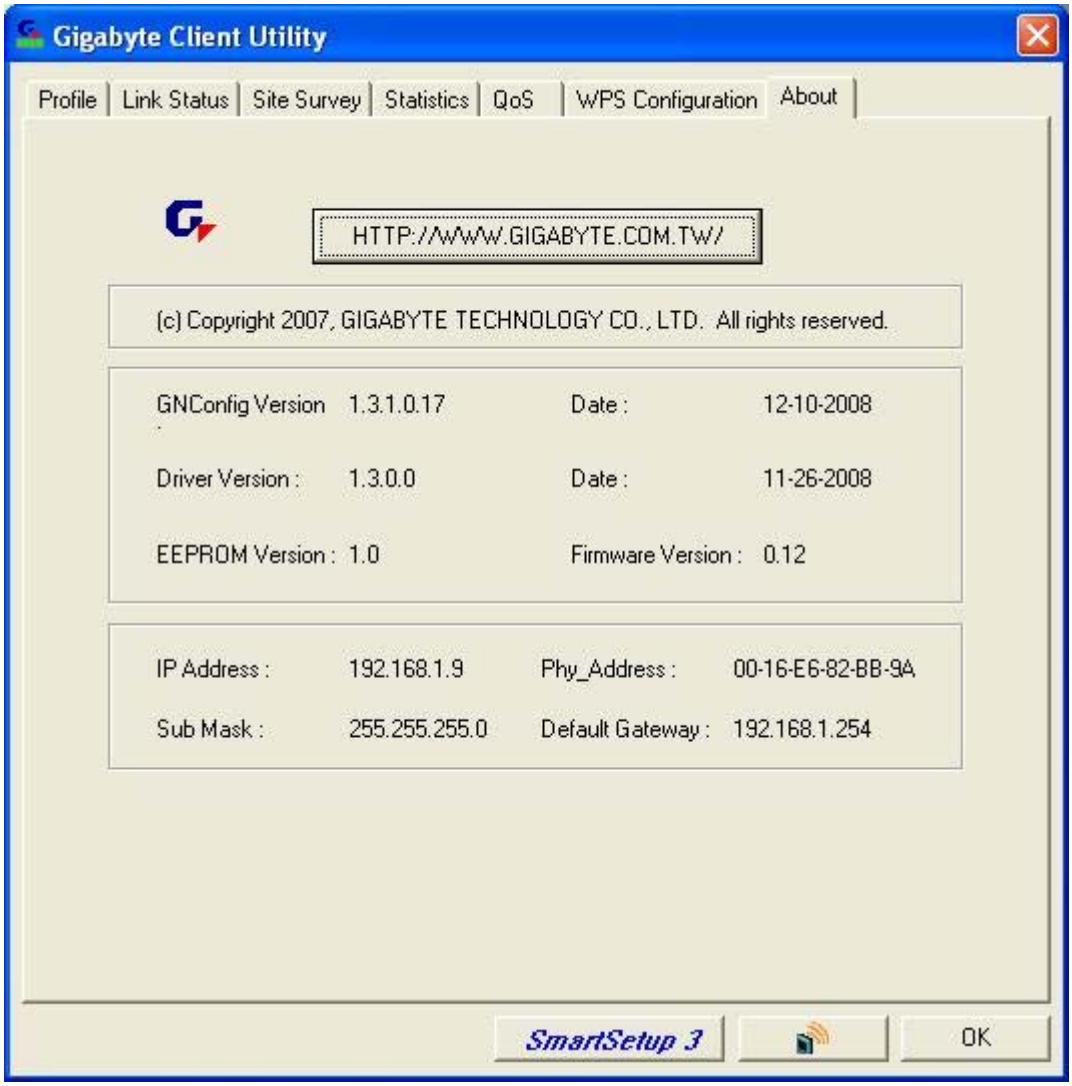

Figure 3-13. About Tab

GNConfig Version (Date) – The version number (and date) of the Adapter Utility

Driver Version (Date) – The version number (and date) of the Adapter Driver.

EEPROM Version – Hardware version number of the Adapter's EPROM**.**

IP Address – The current IP Address of the Adapter.

Phy_Address – The MAC address of the Adapter.

Sub Mask – The current Subnet Mask of the Adapter.

Default Gateway – The current IP Address of the Gateway (typically the IP address of the AP).

Chapter 4 Using Gigabyte Soft AP

4.1 Start Gigabyte Soft AP

Step 1. To start Gigabyte Soft AP, right click the quick start icon located in your system tray and select "**Switch to AP Mode"** or "**Switch to Station Mode".**

Figure 4-1. Switch to AP Mode

Step 2. Switch to AP mode, system will display default information.

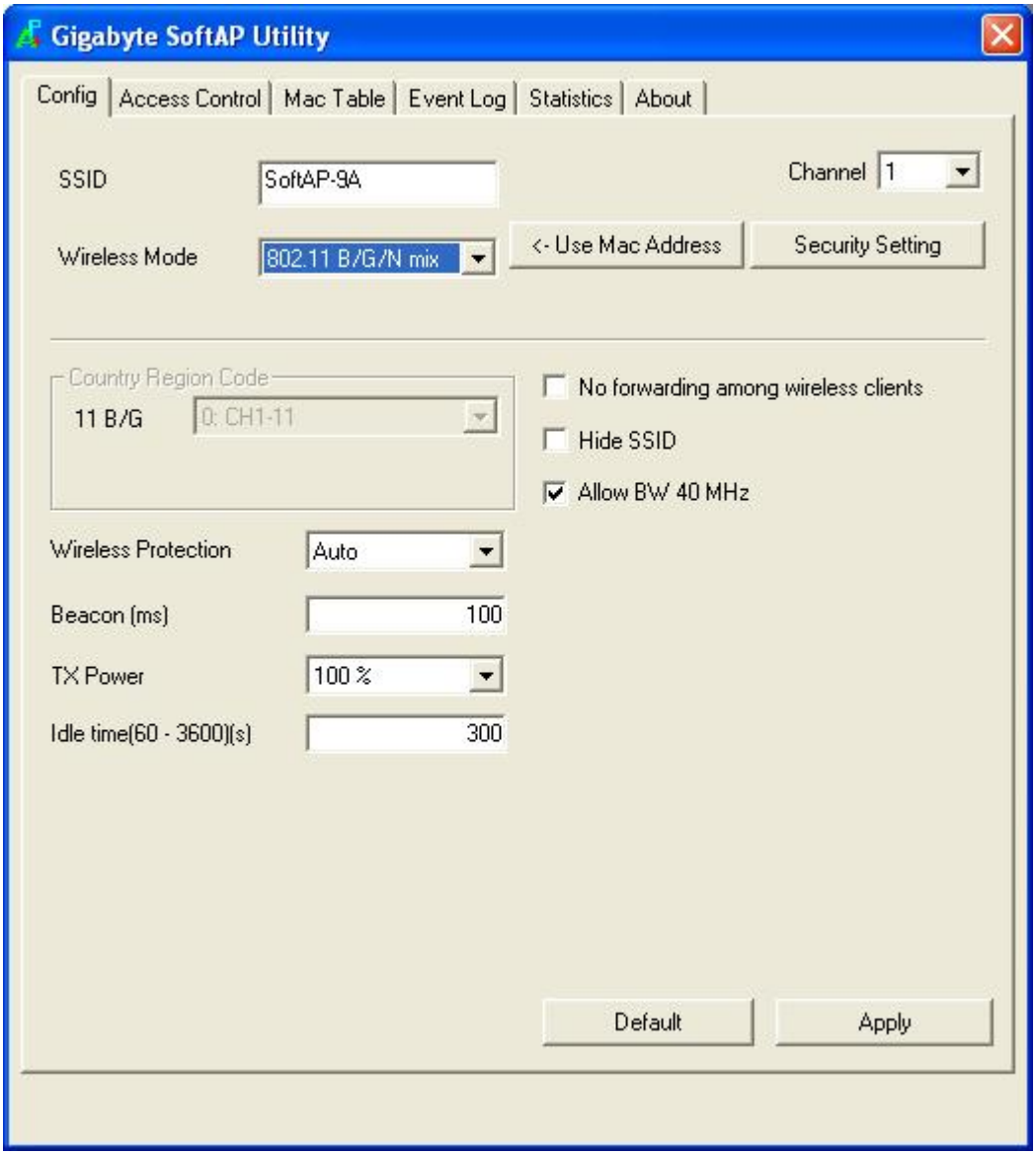

Figure 4-2. Gigabyte SoftAP Utility

At the mean time of starting GNConfig, there is also a small Gigabyteicon appears within

windows taskbar as figure 4-3. You may double click it to bring up the main menu if you selected to close GNConfig menu earlier. You may also use mouse right button to close GNConfig utility.

Figure 4-3. Gigabyte SoftAP Icon

4.2 Config Setting

This page provides configuration setting and display Soft AP detail information.

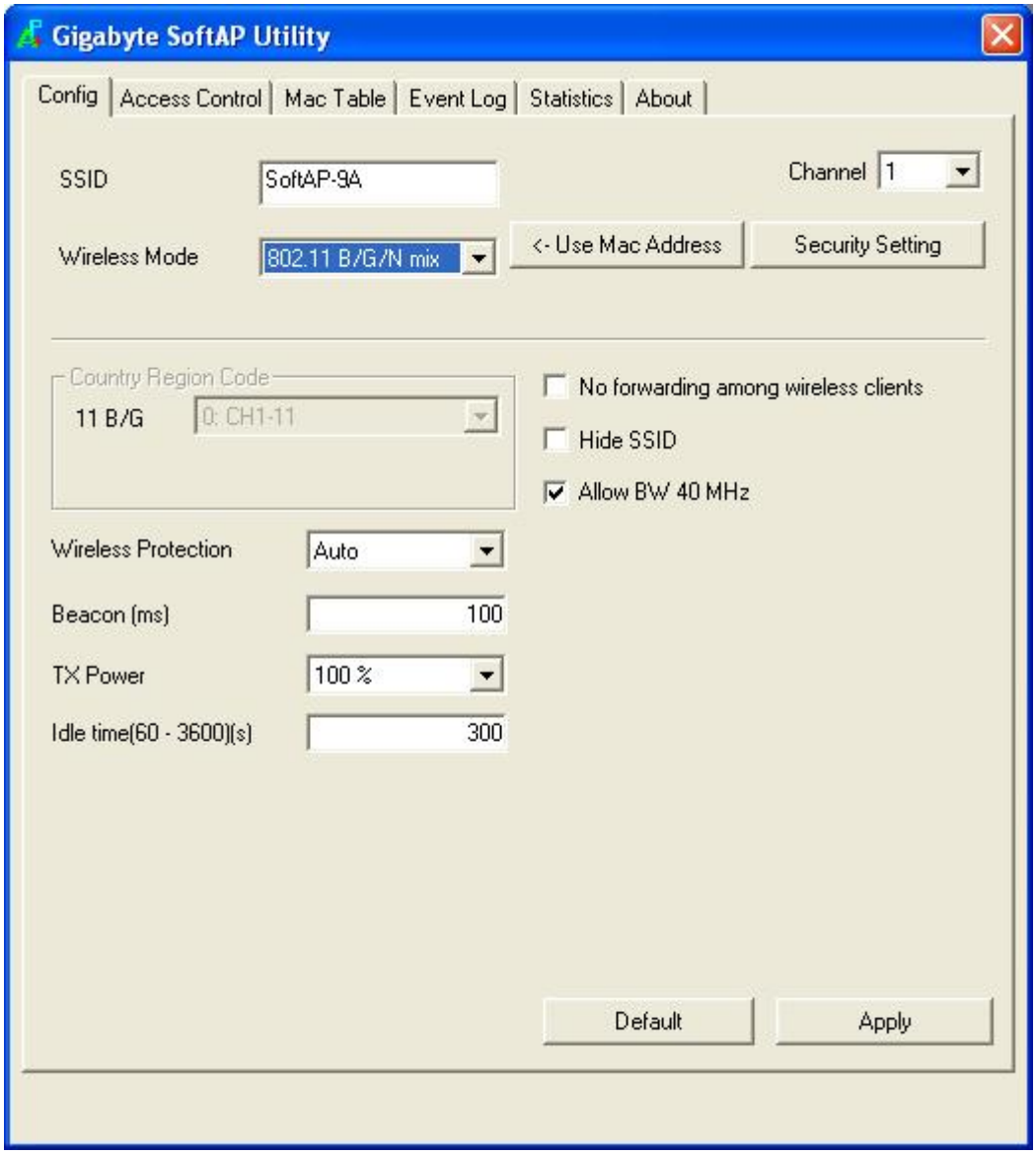

Figure 4-4. Gigabyte SoftAP Utility – Config Window

Description of each field:

SSID–AP name of user type. User also can select [Use Mac Address] to display it. System default is SoftAP-5F.

Wireless Mode– Select wireless mode. Options: 802.11 B/G mix, 802.11B only, 802.11A only, 802.11G only, 802.11 B/G/N mix and 802.11 A/N mix mode are supported. When your wireless card supports 802.11N, the default setting is 802.11 B/G/N mix; Otherwise default setting will be 802.11 B/G mix. (802.11 B/G/N mix selection item only exists for B/G/N adapter)

Wireless Protection– Select the Wireless Protection mode. Options: Auto, on, and off. System default is auto.

a. Auto: STA will dynamically change as AP announcement.

b. On: Always send frame with protection.
c. Off: Always send frame without protection.

Beacon (ms)– The time between two beacons. Default setting is 100 ms.

TX Power– Manually force the AP transmits power. Default setting is 100%.

TX Rate– Manually force the Transmit using selected rate. Default is auto.

Idle Time– Manually force the Idle Time using selected value. Default setting is 300.

Channel– Manually force the AP using the channel. Default setting is channel 1.

Use Mac Address– Use MAC address of used wireless card to be AP name. Default seting is APX. (X is last number of Mac Address.)

Security Setting– Authentication mode and encryption algorithm used within the AP. Default setting is no authentication and encryption. See further section for detail configuration of security.

No forwarding among wireless clients– No beacon among wireless client, clients can't share information within connected Network area. Default setting is no forwarding.

Hide SSID– Hidden AP name. Default setting is no hide.

Allow BW40 MHz– Allow BW40 MHz capability.

Default– Apply system default value.

Apply– Apply the above changes.

4.3 Security Setting

This page can configure security setting and display Soft AP detail information.

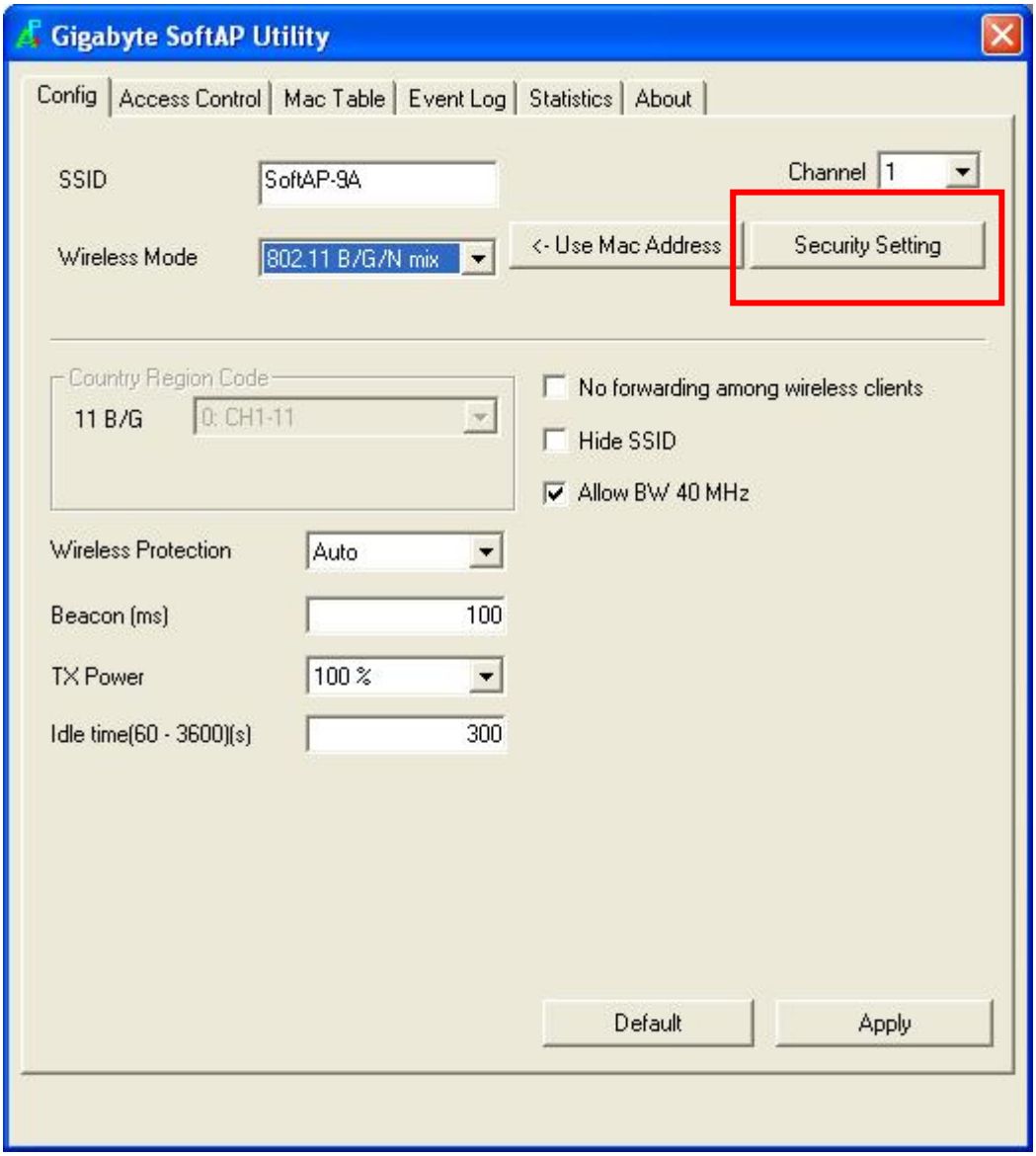

Figure 4-5. Gigabyte SoftAP Utility – Config Window

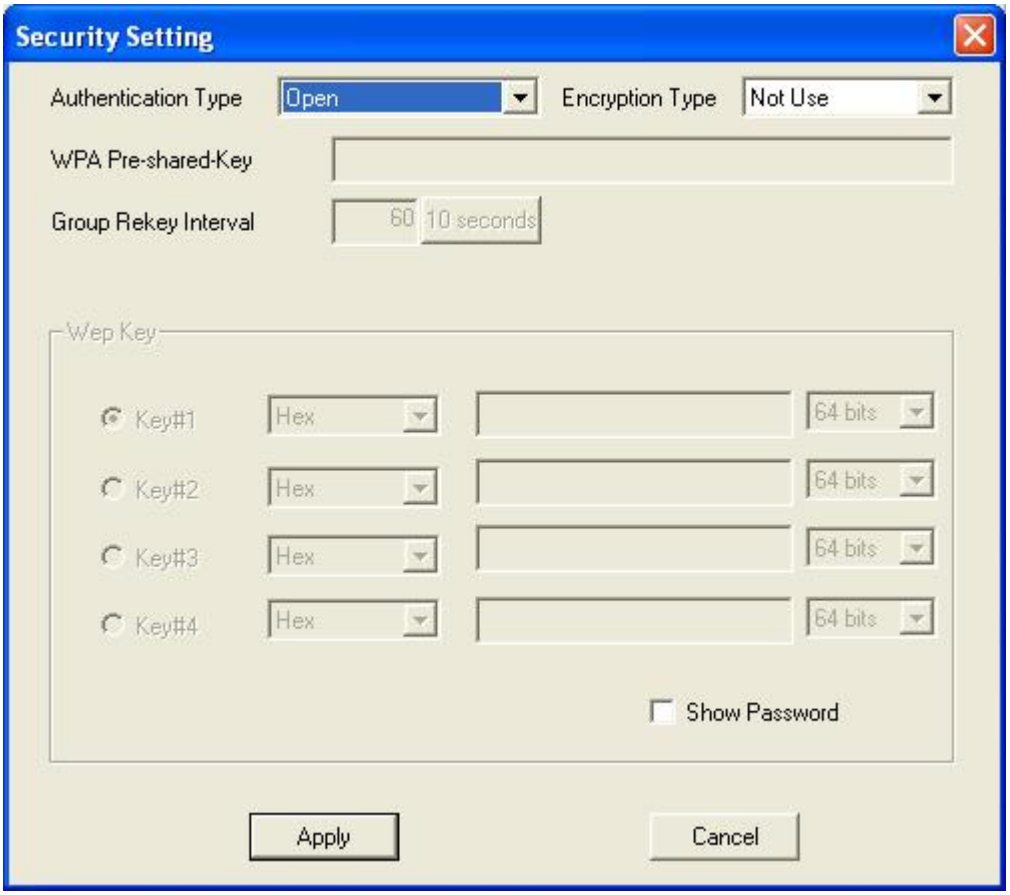

Figure 4-6. Gigabyte SoftAP Utility – Security Setting Window

Description of each field:

Authentication Type– There are three type of authentication modes supported by GNConfig. They are open and WPA-PSK system.

Encryption Type– For open and Share authentication mode, the selected of encryption type are none and WEP. For WPA-PSK authentication mode, the encryption types are TIKP and AES.

WPA Pre-shared Key– This is the shared secret between AP and STA. For WPA-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length. (PCI only)

Group Rekey Interval– Only valid when using WPA-PSK encryption algorithm. The key will change compliance with seconds or beacon that user set. (PCI device only)

WEP Key– Only valid when using WEP encryption algorithm. The key must matched AP's key. There are several formats to enter the keys.

a. Hexadecimal (40bits): 10 Hex characters.
b. Hexadecimal (128bits): 32Hex characters.
c. ASCII (40bits): 5 ASCII characters.
d. ASCII (128bits): 13 ASCII characters.

4.4 Access Control

This page is user setting for AP connection or disconnection with Mac address.

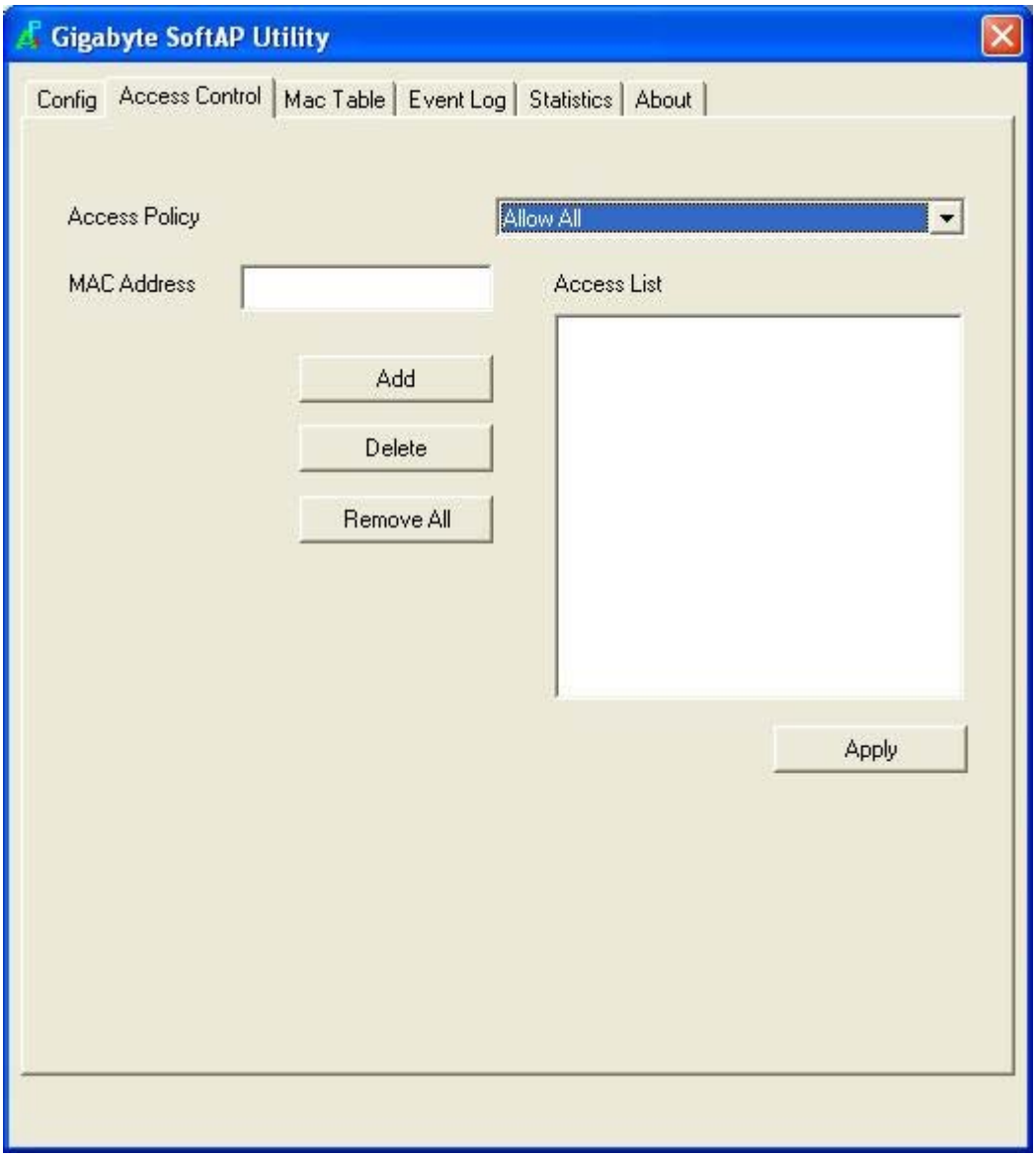

Figure 4-7. Gigabyte SoftAP Utility –Access Panel Window

Description for each field:

Access Policy– Select whether AP start the function. System default is disabling.

Mac Address– Manually force the Mac address using the function, and press [Add] to [Access List].

Access List– Display all Mac Address.

Delete– Delete Mac address.

Remove All– Remove all Mac address in [Access List].

Apply– Apply the above changes.

4.5 Mac Table

Mac Table window displays the station detail information of current AP connection.

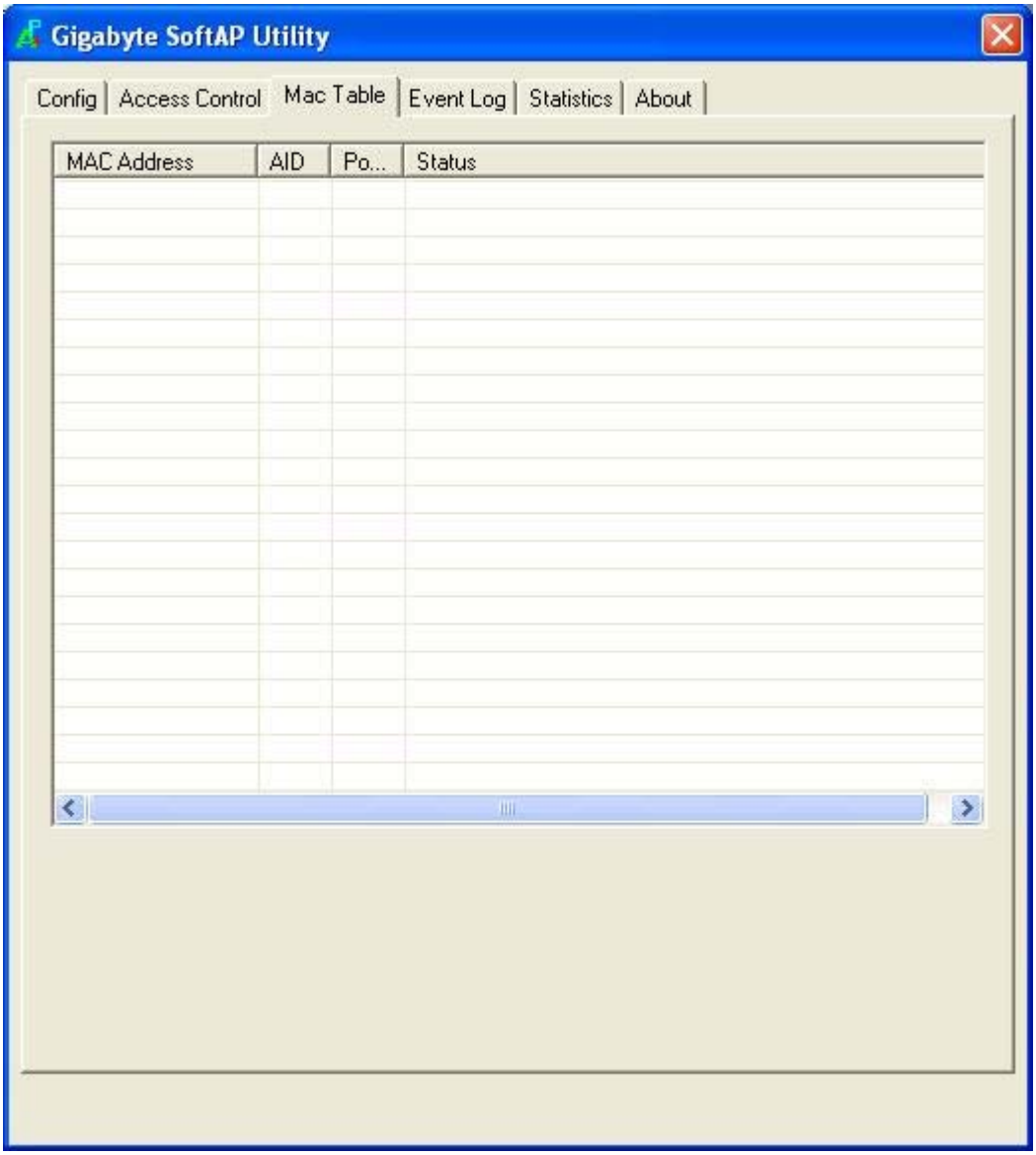

Figure 4-8. Gigabyte SoftAP Utility –Mac Table Window

MAC Address– The station's Mac address of current connection.

AID– Raise value by current connection.

Power Saving Mode– Determine the station of current connect whether support Power Saving Mode.

Status– Displays current AP connection status.

4.6 Event Log

This page log and display Soft AP all event time and message.

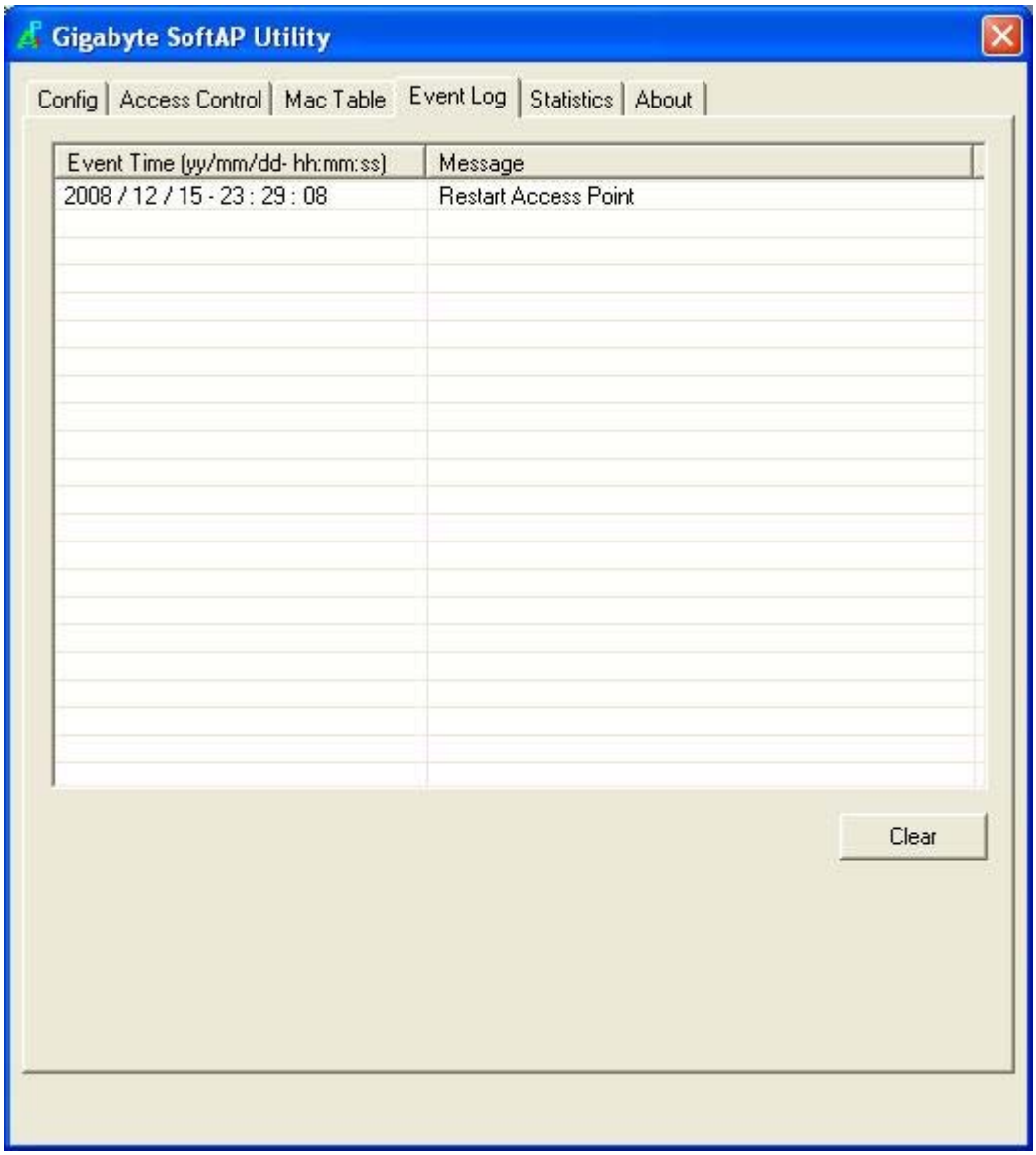

Figure 4-9. Gigabyte SoftAP Utility –Event Log Window

Event Time (yy/mm/dd-hh:mm:ss) – Log event time.

Message– All event message.

4.7 Statistic

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for user to understand.

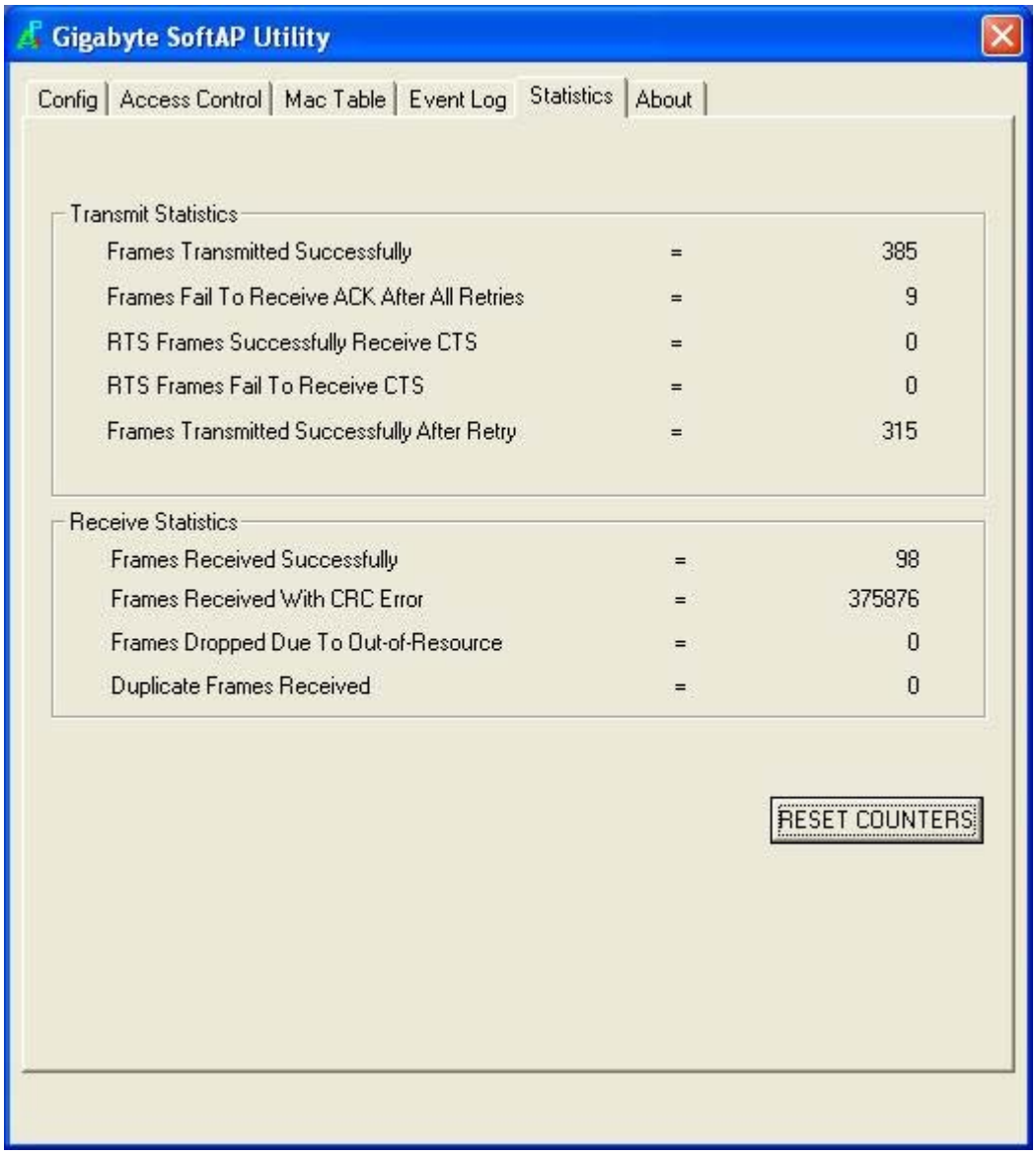

Figure 4-10. Gigabyte SoftAP Utility –Statistics Window

Statistics Transmit:

Frames Transmitted Successfully– Frames successfully sent.

Frames Fail To Receive ACK After All Retries– Frames failed transmit after hitting retry limit.

RTS Frames Successfully Receive CTS– Successfully receive CTS after sending RTS frame.

RTS Frames Fail To Receive CTS– Failed to receive CTS after sending RTS.

Frames Retransmitted Successfully– Successfully retransmitted frames numbers.

Receive Statistics:

Frames Received Successfully– Frames received successfully.

Frames Received With CRC Error– Frames received with CRC error.

Frames Dropped Due To Out-of-Resource– Frames dropped due to resource issue.

Duplicate Frames Received– Duplicate received frames.

4.8 About

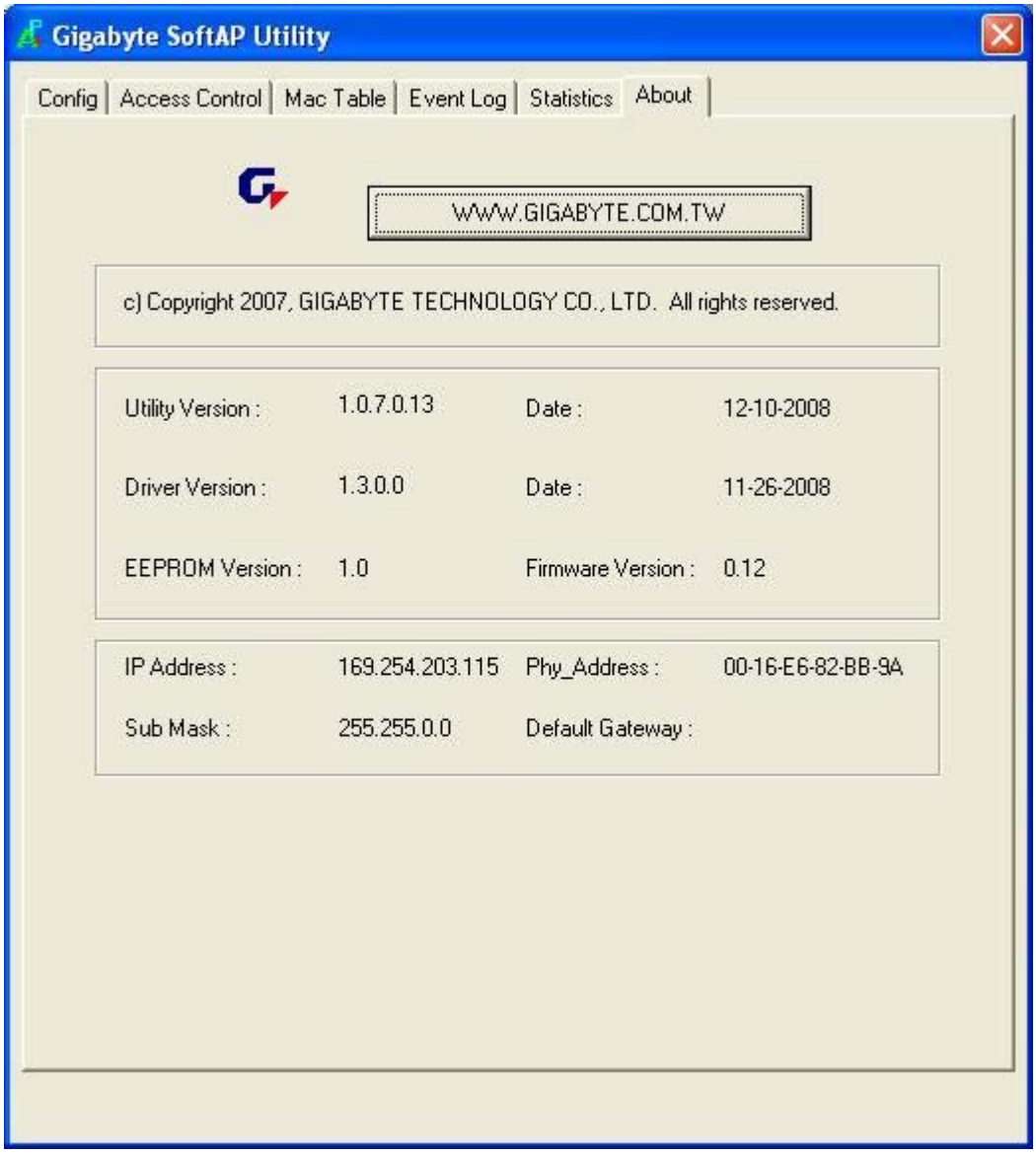

Figure 4-10. Gigabyte SoftAP Utility –About Window

This page display the wireless card and driver version information.

Connect to Gigabyte website: Gigabyte Technology, CO., LTD

Display Configuration Utility, Driver and EEPROM version information.
Display Wireless NIC MAC address.

Appendix A Troubleshooting

This troubleshooting guide provides answers to some common problems which you may encounter while installing or using GIGABYTE Wireless Adapters. Contact the GIGABYTE Wireless Technical Support Team at www.giga-byte.com if you encounter problems not mentioned in this section.

Problem: Cannot connect to an AP
Advice:

- Make sure the SSID for the USB Adapter is the same as the Access Point.
- Make sure the security settings are the same as that of Access Point. When WEP or WPA encryption is enabled, check if the WEP or WPA keys for the USB Adapter and AP are the same.
- Make sure if the MAC address of the Adapter is added in the AP Authorization Table.

Problem: Can connect to an AP but cannot connect to the Internet
Advice:

- Make sure the security settings are the same as that of Access Point. When WEP or WPA encryption is enabled, check if the WEP or WPA keys for the USB Adapter and AP are the same.
- Make sure the network configuration (IP address, subnet mask, gateway, and DNS) of your computer are correct.
- Check the proxy server of the WEB browser is correctly set.

Problem: Poor link quality and signal strength
Advice:

- Keep the Adapter away from microwave ovens and large metal objects to avoid radio interference.
- Keep the distance between the Adapter and the AP as close as possible.

Please check www.giga-byte.com for more complete and up to date troubleshooting tips.

Appendix B
Regulatory Information

CE Mark Warning: This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

Reorient or relocate the receiving antenna.
Increase the separation between the equipment and receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Europe - Declaration of Conformity

CE	This device is a 2.4 GHz low power RF device intended for home and office use in EU and EFTA member states. In some EU / EFTA member states some restrictions may apply. Please contact local spectrum management authorities for further details before putting this device into operation.

GIGA-BYTE Technology, Inc. declares that the product: Wireless USB Adapter Model Number: GN-WS33N-RH is in conformity with and in accordance with the European Directive of EMC, 2004/108/ EC for the following sections:

EN 61000-3-2, EN 61000-3-3, EN 55024, and EN 55022 Disturbances and Immunities

GIGA-BYTE Technology, Inc. also declares the conformity of above mentioned product with the actual required safety standards in accordance with LVD Directive 2006/95/EC:

EN 60950 Safety

In accordance with R&TTE Directive 1995/5/EC, Part 17: Requirements for Operation in the European Community, GIGA-BYTE Technology, Inc declares the conformity of the above mentioned products for:

EN 300 328-2 V1.2.1, ETSI EN 300 328-1：V1.3.1, EN 301 489-1, and EN 301 489-17 Technical Requirements for Radio Equipment

Countries of Operation and Conditions of Use in the European Community
The user should run the configuration utility program provided with this product to check the current channel of operation and confirm that the device is operating in conformance with the spectrum usage rules for European Community countries as described in this section. European standards dictate a maximum radiated transmit power of 100mW EIRP and a frequency range of 2.400 - 2.4835 Ghz.

Appendix C
Warranty

Limited Warranty Statement (1-Year Warranty)

Thank you for purchasing the GIGABYTE Product. This limited warranty statement will provide you one year warranty starting from the purchase date. Of which if any defect is occurred due to accidents or any man-made factors, or any unauthorized torn-off or damage to GIGABYTE's sticker on the product, GIGABYTE Technology will not provide after-sale services, such as:

- Products are damaged due to any violation of instructions on user manual.
- Hardware is damaged due to inappropriate assembling.
- Products are damaged due to the use of illegal accessory.
- Products are damaged due to parts disassembling without authorization.
- Products are damaged due to exceeding environment limits.
- Products are damaged due to unexpected external force.
- Products are damaged due to nature disasters.
- Products are copies or illegally smuggled goods.

PLEASE RECORD THE FOLLOWING INFORMATION REGARDING YOUR WARRANTY

Name of Customer:	
Phone No:	
Address:	
Email:	
Model:	
Serial:	
Date of Purchase:	
Place of Purchase:	
From Whom:	
Distributor:	

Customer Service

GIGA-BYTE TECHNOLOGY CO., LTD.
No.6, Bau Chiang Road, Hsin-Tien,
Taipei Hsien, Taiwan.
Tel: 886-2-8665-2665 Fax:886-2-8912-4007
http://www.gigabyte.com.tw